PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

PERFIL DEL TRABAJO PREVIO LA OBTENCION DEL TÍTULO DE:

MASTER EN REDES DE COMUNICACIÓN

TEMA:

"DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE TRANSICIÓN DE DIRECCIONAMIENTO IPV4 A IPV6 EN LA RED DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO"

JUAN CARLOS DOMÍNGUEZ AYALA

Quito – 2017

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO 1

1.1.Introducción

Con la intención de responder a los retos de tendencias globales existentes (IoT, SDx, BYOD, etc.), en relación a las redes de comunicaciones, la Universidad Politécnica Salesiana (UPS) enfrenta diferentes necesidades y requerimientos dentro de la infraestructura tecnológica actual, mismas que representan una oportunidad de mejora al servicio de la comunidad universitaria.

La Dirección de Tecnologías de la información DTTI ha iniciado la búsqueda de la manera más adecuada de responder a los requerimientos. Se han iniciado estudios que permitan revelar que posibilidades de mejora existen y son alcanzables en un tiempo mediato, la complejidad de la implementación debe ser ajustada para ser ejecutada en un tiempo no mayor de un año.

Estas posibilidades de mejora deben cumplir el propósito de optimización de costos e infraestructura tecnológica.

Se ha escogido como punto de inicio a las mejoras de la red de la UPS sede Quito enfocándose en la implementación del proceso de transición del direccionamiento IPv4 a IPv6.

Con este direccionamiento se procura dar una base para enfrentar los nuevos retos globales de las redes de comunicaciones en la infraestructura actual de la UPS.

Dentro de los retos que se deben llevar en la red de la UPS encontramos:

Una masificación del uso de dispositivos móviles en las aulas de clase, tanto en estudiantes, personal docente y personal administrativo para realizar tareas normales de sus actividades.

Este fenómeno encontrado obedece a las tendencias denominada BYOD (Traer su propio dispositivo) que ha impactado a la red de la UPS en más de una ocasión, superado el número de solicitudes de direccionamiento en cada segmento de red.

Los estudiantes y docentes de la UPS ha incremento el uso de dispositivos raspberry PI y arduinos en proyectos académicos para la simulación de soluciones aplicables en cualquier

campo. También existe una incursión en redes de sensores (WSN, 6LoWPAN), infraestructura fundamentada en software (SDX). Dichos eventos van dando forma a requerimientos hacia la rede de la UPS catalogados dentro de la tendencia denominada el internet de todas las cosas (IoT).

La UPS está proyectando una implementación de consolidación de centros de datos con arquitecturas de referencia (Cisco, NetAPP, VMware) o arquitectura convergente (VCE) que sea parte de una infraestructura de nube hibrida. Por lo tanto, la infraestructura actual debe tener una base de direccionamiento IP adecuada al despliegue de las diferentes infraestructuras de virtualización de escritorios (VDI) y aplicación de red virtual extensible (VXLAN) para los recursos de servidores previstos en la restructuración de centros de datos.

Un adecuado planeamiento del direccionamiento IP brindará el soporte necesario a cualquier implementación de infraestructura tecnológica. Por sus características de escalabilidad, cabecera eficiente, técnicas de transición, etc., el protocolo IP en su versión IPv6 es la base más eficiente para el despliegue de los retos antes mencionados.

1.2.Justificación

El reto que representa este trabajo de maestría es conseguir la migración del protocolo IP de su versión IPv4 a la versión de IPv6, iniciando con estudios teóricos al respecto de IPv6 y culminando con una ejecución planeada y apropiada para garantizar continuidad de las aplicaciones actuales. Este trabajo nos ofrecerá la posibilidad de un adecuado escalamiento de la infraestructura y el soporte a una plataforma global de nuevos retos de Internet.

El planteamiento de la tesis busca resaltar el hecho de que la implementación de IPv6 no solo se refiere a disponer de un direccionamiento escalable y eficiente, sino que también existen otros diferentes tipos de motivaciones para su implementación que se deben considerar, tales como:

- Garantizar la continuidad de las aplicaciones.

- Lidiar con el agotamiento de direcciones IPv4.
- Masificación de dispositivos móviles.
- Retos globales de Internet (Smart Grid, BYOD, WSN, SDX, IoT).
- Entre los beneficios del uso de IPv6 en la infraestructura tecnológica de la red de comunicaciones, podemos mencionaremos los siguientes:
- Mejora en la potencialidad de procesamiento de paquetes en la cabecera IPv6.
- Avances en características de administración debido al direccionamiento IP mejorado y métodos de asignación de direcciones más eficientes.
- Soporte de IP en aplicaciones y funcionalidades para dispositivos móviles.
- Mejora del soporte multicast gracias al aumento de direccionamiento disponible.
- Posibilidad de uso de características de seguridad en IPv6 en la implementación de seguridades de primer salto (FHS).

El proyecto de tesis que se propone en el presente documento se centra en el tema del direccionamiento IPv6 debido a que en el diseño de una red de campus el plan de direccionamiento es una base de fundamental importancia para garantizar el éxito de cualquier implementación de comunicación entre de dispositivos en una red.

La versión actual del direccionamiento IP en la red de la UPS es IPv4. Con la ejecución del estudio de implementación de IPv6 de la presente propuesta, la red de la UPS podrá enfrentar para un proceso adecuado de transición completa de direccionamiento desde la versión IPv4 a la versión IPv6.

En el desarrollo de la documentación de la tesis se describirá el proceso adecuado para mejorar la disponibilidad y servicios de la red a través del cambio nativo del protocolo IP a su versión IPv6.

Entre los elementos involucrados en este diseño, se pondrá atención al ajuste de la estructura nacional de la UPS al direccionamiento jerárquico que permite IPv6. Se diseñará un esquema de direccionamiento que visibilice la estructura administrativa de la sede Quito, los campus que la componen (Girón, Sur y Kennedy) y todas las subredes existentes.

La estrategia de asignación y de administración del direccionamiento IPv6 se realizará a través de métodos dinámicos de asignación de direcciones y ser realizarán pruebas del enrutamiento inter VLAN para las diferentes subredes de los campus y la conexión a Internet.

El proyecto incluye la aplicación de seguridades de la red de la UPS con listas de control de acceso ACL en las áreas funcionales de distribución y frontera para garantizar una correspondencia de las políticas de seguridad establecidas en IPv4 con las nuevas políticas IPv6.

La visibilidad del proceso de transición del direccionamiento IP de IPv4 a IPv6 se logrará con la implementación de un prototipo en la infraestructura actual, en el cual aplicaremos metodologías de diseño fundamentadas en el ciclo de vida de la red y un modelamiento jerárquico empresarial que permitirá la visibilidad total de la infraestructura y los puntos de interacción de las diferentes áreas funcionales para aplicación de seguridades.

1.3.Antecedentes

La Universidad Politécnica Salesiana (UPS) sede Quito está compuesta por los campus Girón (Av. Isabel La Católica N. 23-52 y Madrid), Sur (Rumichaca y Morán Valverde s/n) y Kennedy (Rafael Bustamante s/n).

La UPS sede Quito ha generado para el presente año solicitudes de mejora de toda la infraestructura tecnológica existente. En consecuencia, todas las peticiones de implementación a ser ejecutadas se han planteado como potencialidades de mejora dentro de la planificación institucional. Una de las motivaciones involucradas en la solicitud de mejora de la infraestructura tecnológica está fundamentada en las exigencias de la Secretaria de Educación Superior, Ciencia,

Tecnología e Innovación (SENESCYT), misma que solicita que las Instituciones de Educación Superior (IES) tangan una infraestructura tecnológica funcional al servicio de los estudiantes.

La Dirección Técnica de Tecnologías de Información de la sede Quito (DTTI) al tener como tarea el identifica las necesidades, propone soluciones y las ordena por prioridades, ha elegido al proyecto de direccionamiento IPv6 como el inicio de las mejoras para establecer la nueva plataforma de infraestructura tecnológica de la sede Quito.

En el plan de implementación del proyecto de direccionamiento IPv6, se describirán las estrategias para conseguir la transición del direccionamiento IP actual de versión IPv4, a direccionamiento nativo IPv6, con el objeto de aprovechar todas las ventajas que otorgaría su implementación.

Se diseñará un prototipo que reflejará una correspondencia y transparencia de todas las funcionalidades existentes de la red de campus y de frontera que actualmente se encuentran en IPv4, con la evolución hacia el protocolo IPv6.

1.4.Objetivo General:

Diseño e implementación de un prototipo de transición de direccionamiento IPv4 a IPv6 en la red de la Universidad Politécnica Salesiana sede Quito.

1.4.1. Objetivos Específicos:

1. Evaluar el soporte de la infraestructura actual para el proceso de transición del direccionamiento IPv4 a IPv6.
2. Aplicar un modelamiento jerárquico de red y determinar la metodología que facilite el diseño y el establecimiento de la línea base de la red de la UPS sede Quito.
3. Diseñar el plan IPv6 que permita la salida a Internet de la UPS sede Quito campus Sur, Girón y Kennedy.

4. Implementar un prototipo de transición de direccionamiento IPv4 a IPv6 en las áreas funcionales de red correspondientes a campus y frontera de la UPS sede Quito, Campus Girón.
5. Implementar el prototipo de seguridades con Listas de Control de Acceso (ACL) para IPv6 en la UPS sede Quito, Campus Girón.

CAPÍTULO 2: PROTOCOLO IPV6, MODELOS Y METODOLOGÍAS APLICADAS AL DISEÑO

2.1.Fundamentos del protocolo IPv6.

Los cambios al protocolo IP desde su versión IPv4 a IPv6 fueron necesarios debido al éxito que han tenido los servicios basados en Internet y el consecuente crecimiento exponencial de la demanda de usuarios y de aplicaciones. Desde el año 1990 se hacían públicas las primeras predicciones de que cuatro años más tarde los bloques asignados a usuarios de direcciones IPv4 tipo clase B, se irían agotando lo que motivó el desarrollo de investigaciones que generen estrategias que permitan al protocolo IPv4 soportar las comunicaciones globales del futuro.

Las estrategias generadas fueron: enrutamiento entre dominios sin clase (Clasless Inter Domain Routing CIDR), traducción de direcciones de red (Network Address Translations NAT) y la conformación de segmentos de red pública y privada. Estas estrategias si bien facilitaron la optimización del uso del direccionamiento de IPv4 en las redes también trajeron algunas complicaciones que dieron como resultado que el internet complique su escenario de operación debido que su uso limita el despliegue de nuevas aplicaciones, incrementa el tamaño de las tablas de enrutamiento y limita el soporte para una masificación de dispositivos conectados a internet. Todas estas complicaciones dieron como resultado que las predicciones del uso de IPv4 no sobrepase el año 2011.

En el año de 1998 se libera el RFC2460 con una nueva versión del protocolo IP en versión IPv6, esta versión del protocolo presenta mejoras importantes como: mayor cantidad de direcciones, simplificación de cabecera, métodos de asignación de direcciones, estructura jerárquica de direccionamiento, entre otras.

2.1.1. Mayor espacio de direccionamiento.

IPv6 tiene entre sus diversas mejoras al respecto del protocolo IPv4, una de las más remarcables es que IPv6 ofrece un inmenso número de direcciones superando las limitaciones del protocolo IPv4 de máscara de 32 bits a 128 bits en IPv6.

El soporte de direcciones en IPv4 es $\mathbf{2\ ^{\wedge 32}}$ que da como resultado alrededor de 4 billones de direcciones, en IPv6da la posibilidad de $\mathbf{2\ ^{\wedge 128}}$ que nos un aproximado de 340 sextillones de direcciones posibles.

La cantidad de direcciones disponibles en IPv6 nos brindará un amplio soporte a la evolución de una nueva forma de usar el internet, facilitando la conexión de dispositivos que hasta hoy no se conectan a la red. IPv6 se vuelve clave para facilitar a las redes de comunicación dar soporte y respuesta a las tendencias y retos globales de las redes de datos actuales, donde se destaca el internet de todas las cosas (IoT). Esta tendencia global nos permite ver la evolución del uso del internet en la actualidad y vemos cada vez como una gran cantidad de dispositivos que usamos frecuentemente se conectan a internet para dar solución a necesidades actuales.

2.1.2. Mejora en la cabecera de IP.

Según el RFC 2460 en IPv6 se simplifican algunos campos existentes en IPv4 y otros campos se hacen opcionales, lo que ayuda en la reducción del tiempo de procesamiento y el tamaño de la cabecera lo que nos permite disminuir el costo del ancho de banda de la cabecera IPv6.

En un breve resumen de los principales cambios en IPv6, podemos destacar la gestión de opciones en el campo de nombre “siguiente cabecera”, lo que flexibiliza el desarrollo a nuevas opciones y mejora el manejo del tamaño de la cabecera.

El manejo de la identificación de flujos de información para la aplicación de calidad de servicio en el campo etiqueta de flujo que permitirá especificar el tratamiento que deberá tener cada paquete dependiendo de los requerimientos de cada aplicación.

Por la característica de IPv6 al tener la cabecera de tamaño fijo se añade una estructura de lista enlazada donde se incluye encabezados de extensión que son útiles para añadir distintas funcionalidades cuando sean requeridas entre la cabecera fija y la carga útil.

2.1.3. Seguridad.

La seguridad en IPv6 tiene un componente pensado en la inclusión de características de seguridad nativa a diferencia de IPv4 en el que no se fijó esta característica como una real necesidad, esta característica es otorgada por el uso de IPSec en la gestión segura de las comunicaciones.

La seguridad en IPv6 garantiza la conexión entre dispositivos lo que permite mitigar problemas de seguridad al incluir protección de cifrado y firmas digitales para minimizar la posibilidad de brechas de seguridad en tránsito de la información.

Entre las principales consideraciones al implementar IPv6 están que se trata de un protocolo con muchas posibilidades de aplicaciones futuras como base para el direccionamiento de internet de las cosas (IoT) pero que también hay que considerar que existe poca experiencia en el uso y la implementación del IPv6 y muchos temas adicionales no tomados en cuenta en seguridad que pueden dejar a la red expuesta a riesgos mayores.

Existen algunas consideraciones al tratar con el aspecto de la seguridad en IPv6 a partir de la implementación, las que se refieren brevemente a continuación:

Ataques de fragmentación: Por la característica de IPv6 de que la información trasmitida solo se ensambla en los dispositivos finales y no en nodos intermediarios este ataque no sería efectivo.

Escaneos de direcciones IP por fuerza bruta: Por la gran cantidad de direcciones existentes en el protocolo IPv6 la posibilidad de éxito es mínima, pero se pueden iniciar procesos para intentar tener éxito considerando las técnicas de asignación de direcciones (uso de palabras, uso de las direcciones más bajas en el direccionamiento).

Ataques de “hombre en el medio” y “denegación de servicio”: Tomando ventaja de las características de SLACC y a través de algunas herramientas se puede conseguir suplantar identidades y obtener información de la red.

2.1.4. Multicast

Multidifusión es una de las características que se usan en los dos protocolos de IP, pero es en la versión de IPv6 que se usa para suplantar las funcionalidades que se realizaban con difusión o broadcast en IPv4. Multicast o multidifusión en IPv6 se usa conjuntamente con ICMP v6 para procesos de autoconfiguración en el direccionamiento, procesos de detección de direcciones duplicadas y resolución de direcciones. Esta característica de multidifusión hace más eficiente el uso de recursos de comunicación. El prefijo de direccionamiento está dentro del rango FF00::/8 A FFFF::/8.

2.1.5. Autoconfiguración

Una de las funcionalidades más destacables en el direccionamiento IPv6 es la facilidad de implementación y asignación de direccionamiento a las interfaces de los nodos de la red. El proceso de auto configuración se lleva a cabo por un proceso de descubriendo de vecinos (ND), con el que verifica la validez de la dirección a través de un proceso complementario de detección de direcciones duplicadas (DAD). En el proceso en cada interface se crea una dirección de enlace local que le permite trabajar dentro del mismo segmento de la red sin la necesidad de una puerta de enlace.

Los dos métodos de asignación automática son los de autoconfiguración sin estado (SLACC) y con estado que es muy similar a la configuración mediante un servidor DHCP en IPv4.

EL método de configuración sin estado SLACC es exclusivo de IPv6 y que permite que el cliente tome su propia dirección con la información del prefijo anunciada en su interface directamente conectada.

2.1.6. Movilidad

La característica de movilidad es un protocolo de comunicaciones diseñado por la IETF ya definido con funcionalidades claras para IPv4, mismo que fue actualizado para IPv6. A través de las características de movilidad se permite a los usuarios moverse de una red a otra manteniendo su dirección IP para que no exista interrupción en la comunicación. Las características principales de la movilidad se asemejan a los conceptos de roaming en redes de telefonía móvil.

2.1.7. Privacidad

La característica de privacidad en IPv6 tiene su aplicación más visible en el soporte de las características de movilidad y está más orientado al uso de extensiones de privacidad que permiten mantener la privacidad de los usuarios de dispositivos móviles. Su intención es la protección de la visibilidad global de los dispositivos y protegerlos contra la trazabilidad en la red con movilidad.

2.2.Estado de IPv6 en América latina y el Caribe.

El direccionamiento de IPv6 tienen una gran adopción en América latina y el Caribe según las estadísticas que se pueden obtener de los sitios de google y de 6lab Cisco, donde se muestra un notable avance en el despliegue, implementación y soporte del direccionamiento IPv6 como se muestra en la figura 1. Las estadísticas arrojan una calificación de 10 puntos en un promedio global. Esta nota, que es la máxima dentro de la escala de calificación, muestra un adecuado y

mayoritario despliegue del direccionamiento IPv6 (con un valor de 10/10). Por otro lado, la ausencia de esfuerzos de implementación de IPv6 tiene un valor de 0/10.

Tabla 1.

Estado de IPv6 en América Latina y el Caribe (Fuente; El autor)

País	**Índice relativo /10**	**Ubicación**
Ecuador	7,1	América del Sur
Perú	5,7	América del Sur
Trinidad y Tobago	5,7	Caribe
Brasil	5,6	América del Sur
Argentina	3,4	América del Sur
Puerto Rico	3,1	Caribe
República Dominicana	3	Caribe
Cuba	2,7	Caribe
Colombia	2,6	América del Sur
Bolivia	2,4	América del Sur
Granada	2,4	Caribe
San Cristóbal y Nieves	2,2	Caribe
Uruguay	2,2	América del Sur
Venezuela	1,9	América del Sur
Paraguay	1,7	América del Sur
Chile	1,5	América del Sur
Jamaica	1,2	Caribe
Bahamas	0,2	Caribe
Haití	0,1	Caribe

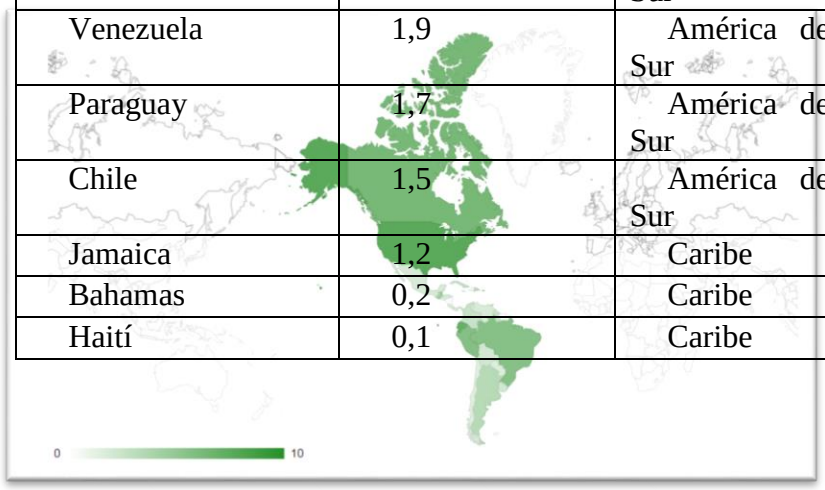


Figura 1. Mapa del estado de IPv6 en América (Fuente; http://6lab.cisco.com)

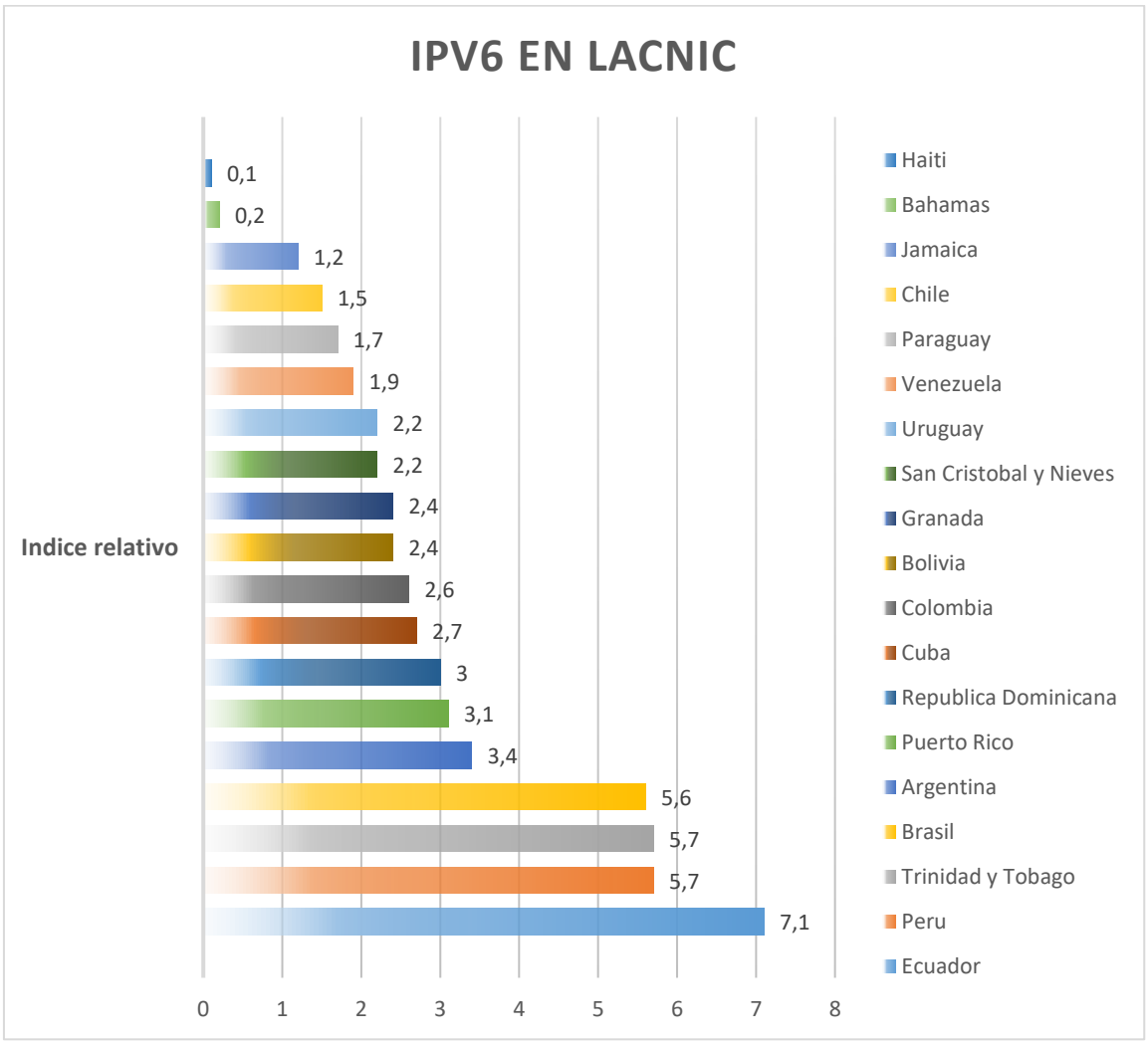


Figura 2. Grafico del estado de IPv6 en América latina y el Caribe (Fuente; El autor)

En la figura 2 destacamos la calificación que tiene Ecuador de 7,1/10 esta calificación es el resultado de la revisión de la cantidad de prefijos IPv6 activos, el contenido disponible en IPv6, los sistemas autónomos disponibles habilitados para transportar IPv6 y la cantidad de usuarios en IPv6 que superan los 2 200 000 usuarios en el país.

2.3.Métodos de transición IPv4 a IPv6

Para el despliegue de transición del direccionamiento IPv4 a IPv6 se establecen tres modelos principales que facilitan el despliegue de IPv6 en la red, los que se describirán brevemente a continuación:

2.3.1. Modelo de doble pila de protocolo (DSM)

Este modelo está basado en la implementación de doble pila de protocolo "dual stack" que consiste en la implementación de los dos tipos de protocolos en la red IPv4 e IPv6, este método de transición facilita la implementación de las características de IPv6, y dejar la infraestructura tradicional de IPv4 trabajando en la red, la convivencia de los dos protocolos en la red de campus es transparente para los usuarios, permite a los clientes acceder a los recursos y servicios de red disponibles en IPv4 y/o en IPv6. Actualmente no todos los servicios de internet y/o aplicaciones más usadas están disponibles para los dos tipos de protocolo IP en v4 y v6 y dependen de características de soporte en hardware y software.

La principal ventaja de DSM y de la implementación de los dos tipos de protocolo de IPv4 e IPv6 en la red es que no se requiere de configuraciones complicadas, ni ningún tipo de características de interpretación o interacción de los protocolos de IP dentro de la red, los protocolos mantienen su independencia en su operación y en las diferentes características de infraestructura de red como es el caso de enrutamiento, seguridad, calidad de servicio, etc.

2.3.2. Modelo híbrido (MH)

El modelo hibrido está compuesto por la implementación de dos o más mecanismos de transición que faciliten el despliegue de IPv6 a medida de la capacidad, aplicaciones y necesidades de la red, los principales métodos de transición y más comúnmente usados son:

Doble pila "dual stack": implementación de IPv4 e IPv6 en la red.

Protocolo automático de direccionamiento de túnel intra-sitio (ISATAP): mecanismo que crea túneles desde los nodos al router que garantiza la implementación de IPv6 dentro de una infraestructura IPv4 en producción.

Configuración manual de túneles: mecanismo que habilita túneles entre routers en infraestructuras de red de IPv4 en producción.

La principal ventaja de implementación del modelo hibrido es la facilidad de la implementación de IPv6 en la red, además permite manejar limitaciones administrativas que se encuentren en la infraestructura actual sin necesidad de actualizaciones o cambio de dispositivos de red. Permite flexibilidad en configuración por facilitar la adopción de los métodos de transición dependiendo de las limitaciones que se encuentren en la red existente.

2.3.3. Modelo bloques de servicio (SBM)

Este modelo es aplicado para la rápida implementación de IPv6 y es una mezcla entre túneles ISATAP, túneles manuales y configuración de doble pila. Este modelo ayuda a la implementación de IPv6 como una infraestructura sobrepuesta que no afecta a la red IPv4 implementada, este modelo depende de características especiales existentes en los switch con controladoras y algunos enrutadores de las series ISR (Router de Servicio Integrado) que soporten la carga del trabajo de los tunes ISATAP para su implementación que hacen el trabajo dinámico de la terminación entre los host con configuración de doble pila de protocolo, El modelo SBM asegura una infraestructura de red de alto rendimiento y con facilidades de crecimiento para toda la red de campus.

La diferencia entre el modelo SBM y HM es que en SBM se usan estos equipos con características de hardware especiales que aseguran una red de alto desempeño y HM usa los equipos actuales para la implementación de IPv6.

2.4.Modelo jerárquico empresarial para diseño de red.

Para la facilidad de la implementación de la infraestructura de red y tener una visibilidad de los puntos de interacción entre los diferentes equipos que componen la red, se utiliza un modelo jerárquico empresarial que organiza la red en módulos con áreas funcionales que describen muy claramente los componentes dentro de la red y la interacción entre cada área y cada equipo, lo que facilita la identificación de equipos de misión crítica, puntos de falla simple y donde se requeriría atención en la implementación de políticas de tráfico y de características de seguridad, la implementación de este modelo nos da una visión más holística de la red la repr4esentacion grafica de este modelo se puede visibilizar en las figuras 3 y 4.

Los módulos que componen a este modelo son:

- Red de Campus
- Frontera de la Empresa
- Frontera del proveedor
- Remoto

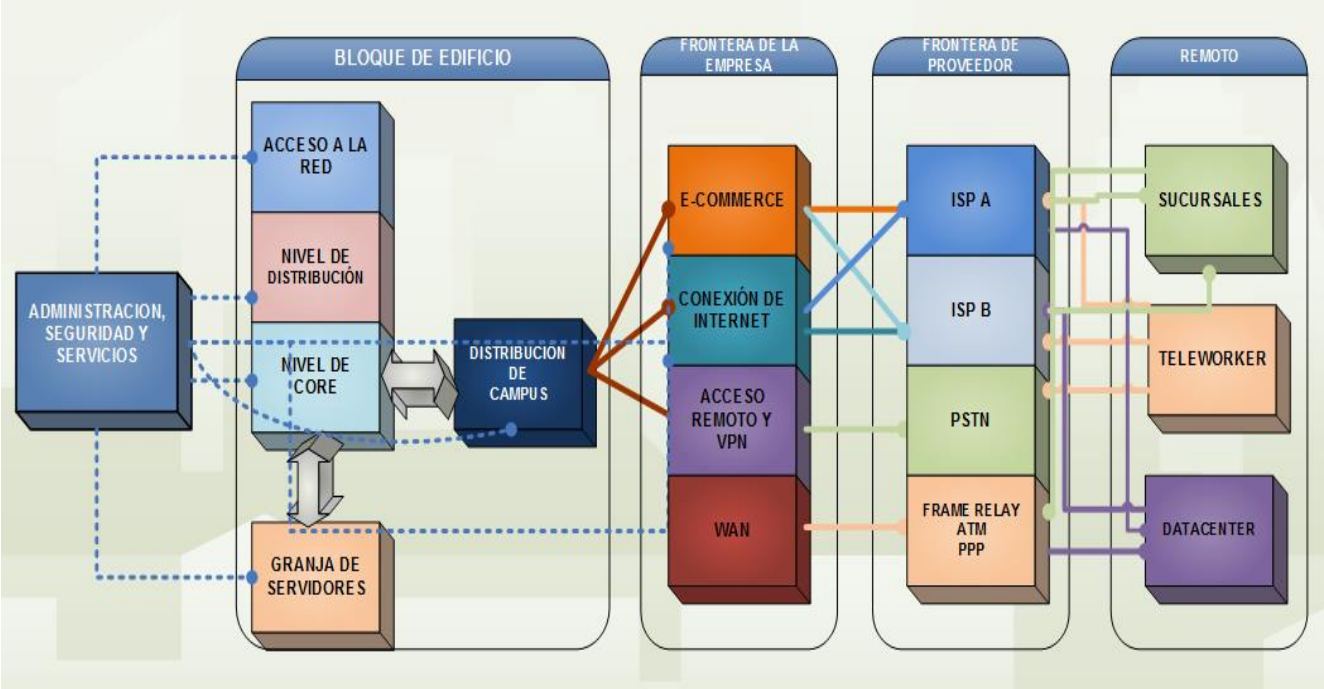


Figura 3. Modelo jerárquico empresarial (Fuente; El autor)

2.4.1. Módulo de red de campus

En este módulo encontramos los componentes que conforman la red de la empresa y tiene como base el modelo tradicional de tres capas acceso, distribución y núcleo, y como complementos importantes de este módulo se encuentran los componentes de granja de servidores, módulo de monitoreo y de servicios.

2.4.2. Módulo de frontera de la empresa

Este módulo nos permite la visibilidad de todas las conexiones que existen de nuestra red con el mundo, está compuesta por las áreas funcionales de e-commerce, acceso a internet, acceso remoto y VPN y WAN, cada una de las áreas funcionales tienen equipos que conectaran, protegerán a la red y filtraran las conexiones del exterior provenientes de la frontera del proveedor.

2.4.3. Módulo de frontera del proveedor

Nos muestra las vías que tiene nuestra red para conectarse a través de los diferentes servicios de un proveedor de servicios (internet, datos y telefonía) que dependiendo de las aplicaciones y de la prioridad tendremos enlaces redundantes a cada una de las áreas funcionales de la frontera de la empresa.

2.4.4. Modulo remoto

Esta área funcional describe la conexión de los recursos que la red empresarial tendrá con ubicaciones geográficamente distantes, trabajo a distancia y nuevas tendencias como centros de procesamiento de datos corporativos en nube. Este módulo facilita establecer los lineamentos mínimos que deberán cumplir las oficinas remotas o sucursales para garantizar acceso a recursos de gestión centralizada y catálogos de aplicaciones, los trabajadores a distancia ingresarán a los recursos disponibles de la red a través de conexiones seguras desde las opciones de conectividad de banda ancha.

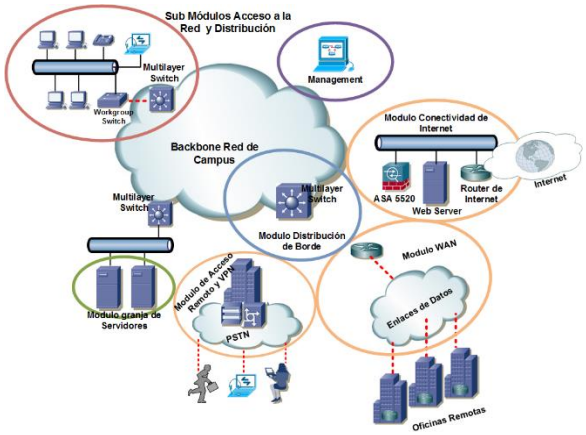
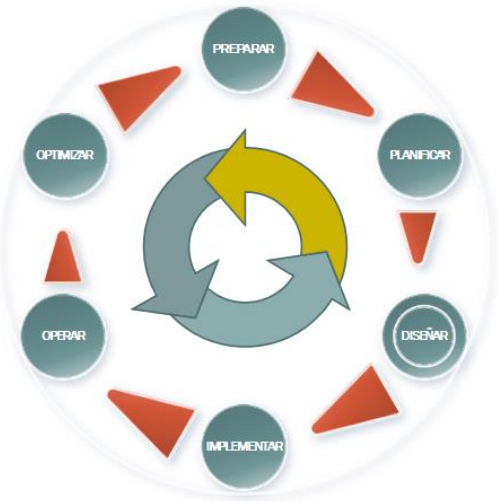


Figura 4. Diagrama lógico modelo empresarial (Fuente; El autor)

2.5.Metodología de Diseño.

La metodología de diseño en la implementación es PPDIOO, esta metodología está fundamentada en el ciclo de vida de la red y sus siglas significan preparación, planificación, diseño, implementación, operación y optimización. El uso de esta metodología nos permite alinear la red a las necesidades del negocio y obtener resultados finales apegados a solucionar los



requerimientos deseados en la red.

Figura 5 Metodología PPDIOO (Fuente; El autor)

2.5.1. Preparar

En esta fase se establece las necesidades y los objetivos del nuevo diseño, se consideran todas las justificaciones para la puesta en marcha del proyecto.

2.5.2. Planificar

Esta fase nos permite analizar todos los requerimientos solicitados a ser cubiertos e implementados bajo las mejores prácticas y recomendaciones.

2.5.3. Diseñar

En la etapa de diseño se puede escoger un modelamiento en capas que asegure que el resultado final sea lo que se había requerido inicialmente. El modelamiento en capas puede referirse a un modelo de referencia como el modelo OSI, o un modelo fundamentado en protocolo como TCP/IP que garanticen que en la etapa de diseño se cubra todos los requerimientos. Las metodologías a escogerse en la etapa de diseño pueden ser el de iniciar desde la capa superior que sería la capa aplicación y terminar en la capa inferior que sería la capa física. A esta opción se la llama “top-down”, la otra alternativa es usar el proceso contrario iniciar desde la capa física y terminar en la capa de aplicación, denominada “buttom-up”.

2.5.4. Implementar

En esta opción se procede con la configuración de la documentación que se ha creado en la etapa de diseño, los técnicos utilizan los planes de implementación y diagramas que fueron creados en el diseño para estimar tiempos de trabajo y otros procesos.

2.5.5. Operar;

La etapa de operación se procede a la puesta en marcha de la infraestructura, y se mantienen continuos procesos de monitoreo y de administración con control de cambios que surjan en la fase de producción.

2.5.6. Optimizar

La fase de optimización está destinada a una gestión proactiva de la infraestructura de red, proponiendo mejoras o correcciones a la infraestructura en producción iniciando nuevamente las fases de preparación y planificación de las mejoras propuestas.

CAPÍTULO 3: CARACTERIZACIÓN DE LA RED ACTUAL

3.1.Campus El Girón.

Este campus se encuentra ubicado en el sector centro norte de la ciudad de Quito en las coordenadas aproximadas de latitud -0° 12′ 29,55”, longitud -78° 29′ 16,55”, y altitud 2850m, tiene dos bloques el bloque A ubicado en Av. 12 de Octubre 2422 y Wilson y el bloque B en la calle Isabel la Católica N23-52 y Madrid.

Para la descripción de la red actual del campus utilizaremos el modelo jerárquico empresarial en el área funcional de red de campus y frontera de la empresa.

3.1.1. Red de campus.

La infraestructura de red del campus El Girón está organizada bajo la configuración de núcleo colapsado (funciones de distribución y núcleo en el mismo equipo) con un equipo Cisco catalyst WS-C6506-E que tiene características redundantes a nivel de controladora (VS-SUP2T-10G) y fuentes de poder (WS-CAC-4000W-US), tiene una configuración de una tarjeta de 48 SFP 1G (WS-X6848-SFP) y una tarjeta de 48 UTP 10/100/1000 (WS-X6848-GE-TX).

Figura 6. Equipo Cisco catalyst WS-C6506-E (Fuente; cisco.com)

Tabla 2.

Componentes del equipo Cisco catalyst WS-C6506-E (Fuente; El autor)

NOMBRE COMPONENTE	DESCRIPCIÓN COMPONENTE	NÚMERO DE SERIE (SN)
WS-C6506-E	"Cisco Systems Inc. Catalyst 6500 6-slot Chassis System"	SN: SAL1650U3PA
WS-X6848-SFP	DESCR: "WS-X6848-SFP CEF720 48 port 1000mb SFP Rev. 3.0"	SN: SAL1701W6UN
WS-X6848-GE-TX	DESCR: "WS-X6848-GE-TX CEF720 48 port 10/100/1000mb Ethernet Rev. 1.0"	SN: SAL1703X6KD
VS-SUP2T-10G	DESCR: "VS-SUP2T-10G 5 ports Supervisor Engine 2T 10GE w/ CTS Rev. 1.4"	SN: SAL1703X7DN
VS-SUP2T-10G	DESCR: "VS-SUP2T-10G 5 ports Supervisor Engine 2T 10GE w/ CTS Rev. 1.3"	SN: SAL16095XW0
WS-CAC-4000W-US"	DESCR: "220v AC power supply 4000 watt 1"	SN: SNI1647BL2W
WS-CAC-4000W-US"	DESCR: "220v AC power supply 4000 watt 1"	SN: SNI1647BL33

El equipo WS-C6506-E es el equipo principal de la red y es donde se encuentra la centralización de la gestión de la red de campus; en este equipo se encuentra toda la configuración de redes de área local virtuales (VLAN), servidor VLAN Trunking Protocol (VTP), enrutamiento, seguridad en la distribución con listas de control de acceso (ACL) y políticas de calidad de servicio (QoS).

Tabla 3.
VLAN en el campus El Girón de la UPS (Fuente; El autor)

VLAN	NOMBRE
1	DEFAULT
3	ADMINISTRATIVA
4	VLAN-RELOJ
6	IPT
7	UPS-NET-ESTUDIANTES
9	VLAN-SALA-INTERNET
10	VIDEO

11	INTERNET
12	IUS
13	SOL
14	INSPECTORIA-ADMINISTRATIVA
16	ABYA-YALA
17	CAMARA-IP
18	LNS
19	INTERNET-TVCABLE
20	VWLC
30	PACKET
71	SRV-3
74	WLC-UBNT
99	VLAN0099
100	EVENTOS
112	ADMINISTRATIVOSV2
114	VLAN-WLC
115	VLAN-WLC2
118	IDIOMAS
119	SRV-INTERNOS-V2
120	EVENTOSV2
125	ASA
126	ASA-BC
156	3CX
239	COWORKING
240	ESTUDIANTES-V2
500	CSRFPV2
700	DOCENTES/23
704	CECASIG
708	CENTRO-MULTIMEDIAL
710	DOCENTES
711	SALA-INTERNET
81	SERVIDORES-INTERNOS

0	
820	SERVIDORES-PUBLICOS
830	SERVIDORES-PROXY
840	PROXIM
999	TELCONET

Tabla 4.
Direcciones IPv4 en las interfaces del equipo WS-C6506-E (Fuente; El autor)

VLAN	IP-ADDRESS	STATUS
VLAN 1	172.17.0.1	UP
VLAN 2	UNASSIGNED	DOWN
VLAN 3	172.17.3.252	UP
VLAN 4	172.17.9.62	UP
VLAN 5	UNASSIGNED	DOWN
VLAN 6	172.17.6.254	UP
VLAN 7	172.17.123.254	UP
VLAN 8	UNASSIGNED	DOWN
VLAN 9	172.17.13.126	UP
VLAN 10	172.17.1.126	UP
VLAN 11	UNASSIGNED	UP
VLAN 12	172.17.70.254	UP
VLAN 13	172.17.15.254	UP
VLAN 14	172.17.10.126	UP
VLAN 15	UNASSIGNED	DOWN
VLAN 16	172.17.72.254	UP
VLAN 17	172.17.73.254	UP
VLAN 18	UNASSIGNED	DOWN
VLAN 30	UNASSIGNED	DOWN
VLAN 70	UNASSIGNED	DOWN
VLAN 71	172.17.71.254	UP
VLAN 74	172.17.74.254	UP
VLAN 100	172.17.101.254	UP
VLAN 112	172.17.113.254	UP
VLAN	172.17.114.	UP

114	254	
VLAN 115	172.17.115.254	UP
VLAN 116	172.17.117.254	DOWN
VLAN 118	172.17.118.254	UP
VLAN 119	172.17.119.254	UP
VLAN 120	172.17.124.254	UP
VLAN 125	172.17.125.254	UP
VLAN 126	172.17.126.254	UP
VLAN 156	172.17.156.254	UP
VLAN 239	172.17.239.254	UP
VLAN 240	172.17.247.254	UP
VLAN 500	192.168.25.1	UP
VLAN 700	172.17.201.254	UP
VLAN 704	172.17.5.254	UP
VLAN 708	172.17.8.254	UP
VLAN 710	172.17.11.254	DOWN
VLAN 810	172.17.1.30	UP
VLAN 830	172.17.1.94	UP

Los equipos que se encuentran en la capa de acceso configurados con funciones únicamente de capa 2 (L2) son los modelos de las familias de Cisco catalyst 4507R, 3750, 3750v2 y 2960(S/X) que son equipos de grupo de trabajo, distribuidos por los diferentes cuartos intermediarios y secundarios de cableado estructurado (IDF/SDF). En estos equipos encontramos configuraciones de características de apilamiento de switch (stack), VTP, agregación de links (Ether-Channel), energía a través de ethernet (PoE) y características de QoS.

Figura 7. Equipo Cisco catalyst 4507-R (Fuente; cisco.com)

Figura 8. Equipo Cisco catalyst 3750/3750v2 (Fuente; cisco.com)

Figura 9. Equipo Cisco catalyst 2960(S/X) (Fuente; cisco.com)

El cableado estructurado del campus El Girón está compuesto por cable UTP en cableado horizontal de categoría 6 y cableado vertical en fibra óptica, los cuartos intermediarios y secundarios se conectan con cableado estructurado vertical al cuarto principal donde se tiene categoría 6A para el cableado horizontal en el centro de procesamiento de datos del campus.

Tabla 5.
Plataformas conectadas en la red de campus bloque A (Fuente; El autor

DISPOSITIVO	PLATAFORMA
MDF-B	WS-6506
MDF-B	WS-6507
SDF-AF-P3	WS-C2960X-GIG
SDF-AF-P1	WS-C3750-4GIG
SDF-DECANATOS	WS-C2960X-GIG
SDF-POSGRADOS	WS-C3750-4GIG
SDF-LNS	WS-C3750V2GIG
SDF-DIR.CARRERA	WS-C2960X-GIG
SDF-SECRETARIA	WS-C3750-4GIG
SDF-SECRETARIA	WS-C3750-4GIG
SDF-MULTIMEDIAL-PB.UPS	WS-C3750-4GIG
SDF-UNADEDVI	WS-C2960X-GIG

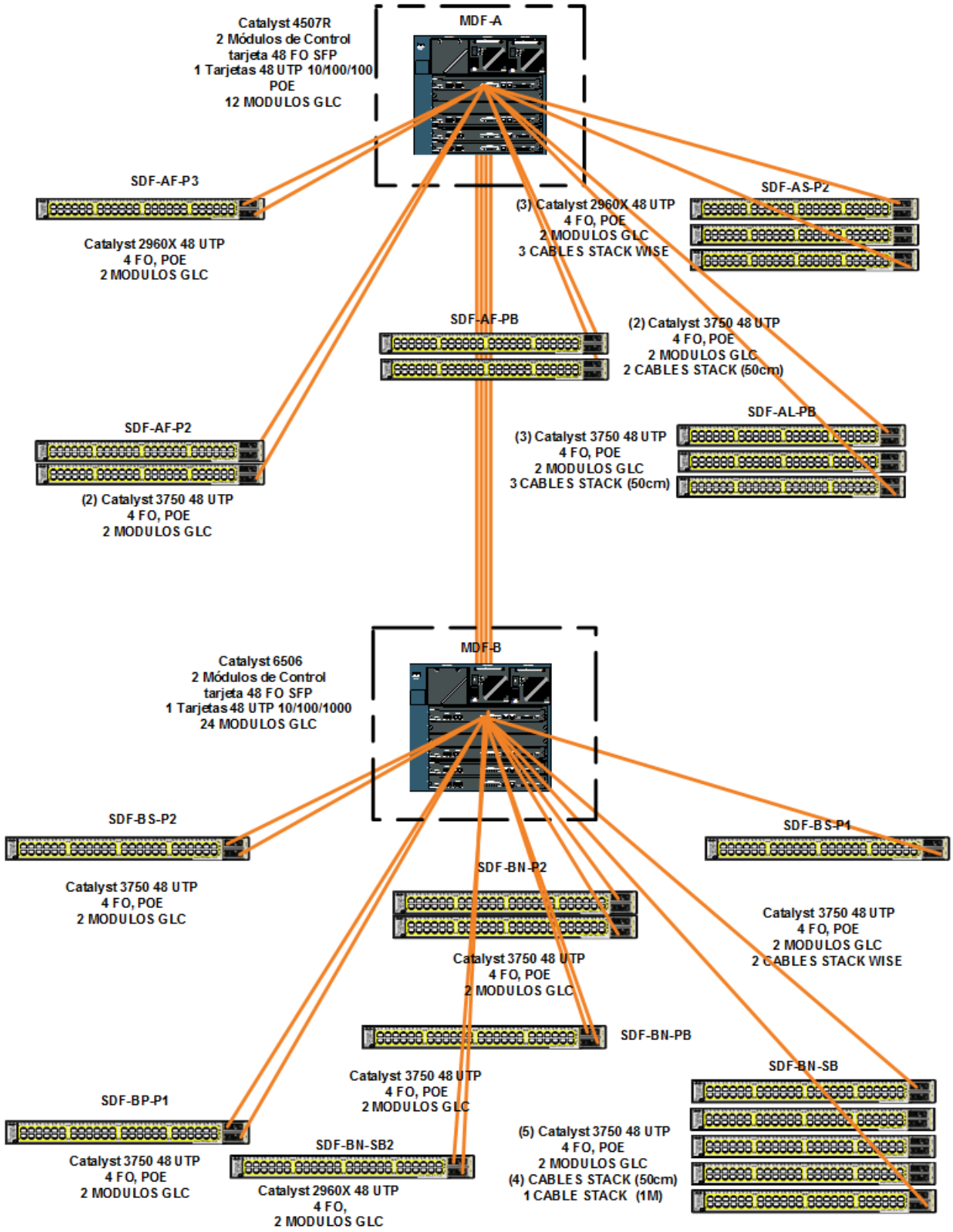


Figura 10. Distribución física de equipos en el campus El Girón de la UPS (Fuente; El autor)

Tabla 6.

Plataformas conectadas en la red de campus bloque B (Fuente; El autor)

DISPOSITIVO	PLATAFORMA
SDF-ADM.EMPRESAS	WS-C3750-
SDF-SERV_APOLLO	WS-C3750G
SDF-SERV_APOLLO	WS-C3750G
SDF-SERV_APOLLO	WS-C3750G
SDF-SERV_APOLLO	WS-C3750G
SDF-AULAMAGNA	WS-C2960-
IDF-A	WS-4507R
IDF-A	WS-4507R
SDF-AULAVIRTUAL	WS-C2960-
SDF-CECASIG	WS-C3750-
SDF-CECASIG	WS-C3750-
RT-UPS-UIOG	CISCO 3825
RT-UPS-UIOG	CISCO 3825
UPS-GIRON.UIO.UPS.EDU.EC	ISR4451-X
MDF-INSPEC	WS-C2960-
IWAN_UPS_GIR.UPS	ISR4451-X
IWAN_UPS_GIR.UPS	ISR4451-X
WLC-UPSG	AIR-CT5508-K9
WLC-UPSG	AIR-CT5508-K9
WLC-UPSG	AIR-CT5508-K9
WLC-UPSG	AIR-CT5508-K9
SDF-BCFP	WS-C3750-
SDF-BIBLIOTECA	WS-C3750-
SDF-BIBLIOTECA	WS-C3750-
SDF-DTIT	WS-C3750V
SDF-PASTORAL	WS-C3750-
SDF-PASTORAL	WS-C3750-

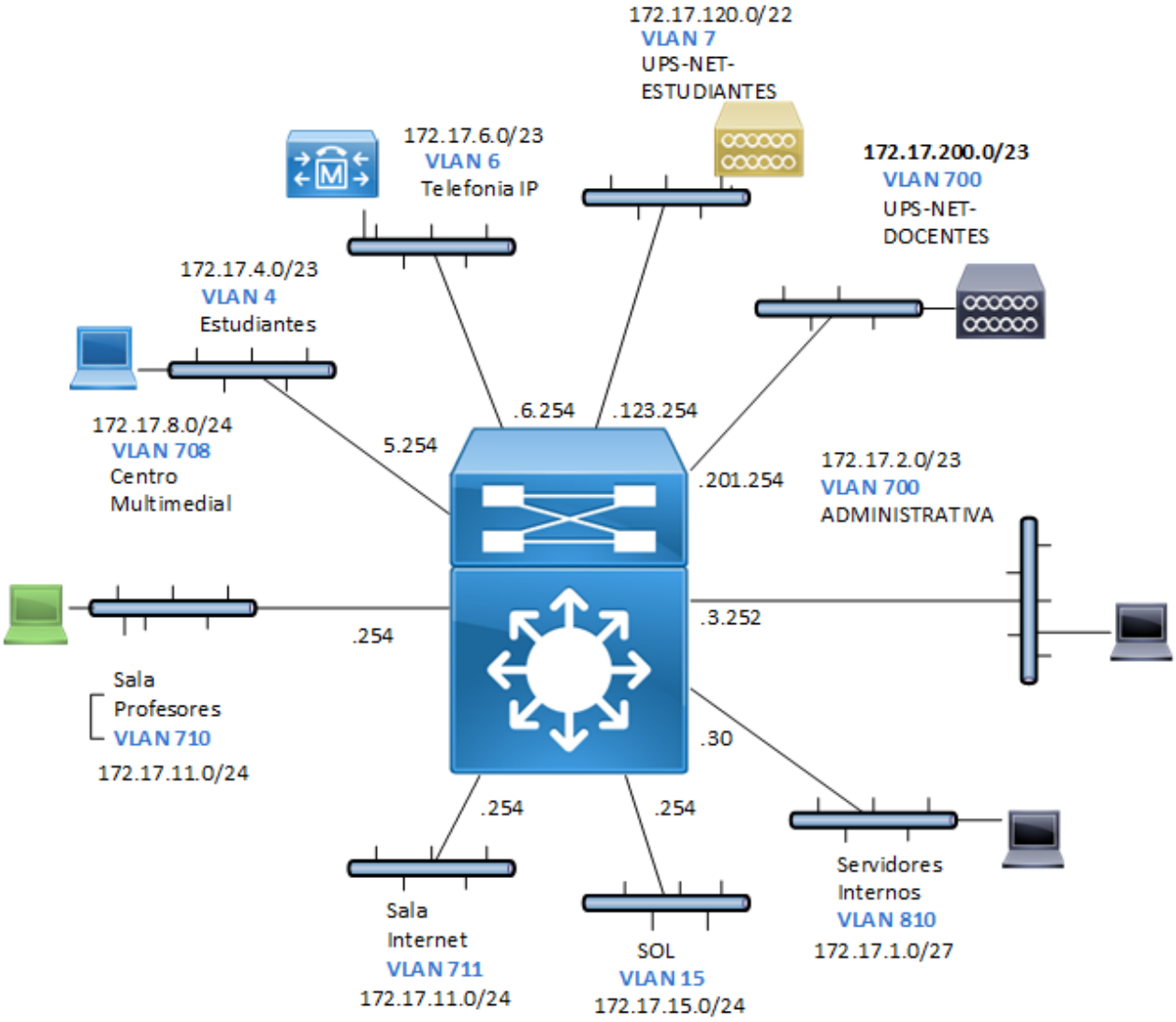


Figura 11. Diagrama lógico red campus El Girón (Fuente; El autor)

Tabla *7.*
Redes IPv4 en campus El Girón (Fuente; El autor)

VLAN	NOMBRE	RED IPV4
1	DEFAULT	172.17.0.0/24
3	ADMINISTRATIVA	172.17.2.0/23
4	VLAN-RELOJ	172.17.9.0/26
6	IPT	172.17.6.0/23
7	UPS-NET-ESTUDIANTES	172.17.120.0/22

9	VLAN-SALA-INTERNET	172.17.13.0/25
10	VIDEO	172.17.1.96/27
11	INTERNET	NA
12	CSRFP	172.17.70.0/24
13	SOL	172.17.15.0/24
14	INSPECTORIA-ADMINISTRATIVA	172.17.10.0/25
15	ADB	NA
16	ABYA-YALA	172.17.72.0/24
17	CAMARA-IP	172.17.73.0/25
18	LNS	NA
19	INTERNET-TVCABLE	NA
20	VWLC	NA
24	VLAN0024	NA
30	PACKET	NA
71	SRV-3	172.17.71.0/24
74	WLC-UBNT	172.17.74.0/24
99	VLAN0099	NA
99	TELCONET	NA
100	EVENTOS	172.17.100.0/23
112	ADMINISTRATIVOSV2	172.17.112.0/23
114	VLAN-WLC	172.17.114.0/24
115	VLAN-WLC2	172.17.115.0/24
116	PRUEBAS	172.17.116.0/23
118	IDIOMAS	172.17.118.0/24
119	SRV-INTERNOS-V2	172.17.119.0/24
120	EVENTOSV2	172.17.124.0/24
125	ASA	172.17.125.0/24
126	ASA-BC	172.17.126.0/24
156	3CX	172.17.156.0/24
239	COWORKING	172.17.239.0/24
240	ESTUDIANTES-V2	172.17.247.240/20
500	CSRFPV2	192.168.25.0/24

700	DOCENTES/23	172.17.200.0/24
704	CECASIG	172.17.4.0/24
708	ENTRO-MULTIMEDIAL	172.17.8.0/24
710	DOCENTES	172.17.11.0/24
711	SALA-INTERNET	NA
810	SERVIDORES-INTERNOS	172.17.1.0/27
820	SERVIDORES-PUBLICOS	NA
830	SERVIDORES-PROXY	172.17.1.64/27
840	PROXIM	NA

3.1.2. Red de frontera.

La red de frontera del campus El Girón está compuesta por toda la infraestructura de conexión con los recursos externos, describiremos brevemente la protección de conexión a internet, acceso remoto VPN y WAN.

3.1.2.1. Conexión de Internet

En esta área funcional se gestiona el acceso a internet y la infraestructura que permite una navegación segura y controlada. Entre el conjunto de equipos que son pate de la infraestructura de frontera están un equipo firewall adaptivo de seguridad de siguiente generación (NGFW) Cisco ASA 5545, encargado de la gestión y administración del aseguramiento de navegación hacia el internet con un complemento de servicio de firePOWER que potencia la robustez de la solución con IPS y protección avanzada contra amenazas.

Figura 12. Equipo Cisco NGFW ASA 5545 (Fuente; cisco.com)

La gestión del filtrado de navegación web está a cargo del dispositivo de seguridad web de nombre Web Security Appliance (WSA) S380, este equipo mantiene la estructura tradicional de filtrado web con características de reputación de sitios web, y un análisis complementario de monitoreo de tiempo real para mitigar problemas de seguridad de la red.

Figura 13. Equipo Cisco WSA S380 (Fuente; cisco.com)

La gestión del ancho de banda y calidad de servicio QoS de internet se realiza a través del equipo de marca Blue Coat PacketShaper 12000 que realiza inspección de paquetes en profundidad a la entrada y salida del tráfico, permitiendo tener una gran visibilidad del consumo de las aplicaciones que usan el servicio de internet.

Figura 14. Equipo Blue Coat PacketShaper 12000 (Fuente; bluecoat.com)

3.1.2.2. Acceso remoto y VPN

En esta área funcional encontramos al equipo Cisco NGFW ASA 5545 con el que gestionamos la posibilidad de conexiones seguras a través de medios públicos como el internet, el NGFW se convierte en un concentrador de VPN facilitando el ingreso externo seguro a los recursos de red disponibles.

3.1.2.3. WAN

Para la conexión del campus con las redes de área extendida utilizamos equipos enrutadores de dos tipos, el equipo Cisco ISR4451-X es el router principal que cumple funciones de gateway de voz, tiene las configuraciones de gestión de enrutamiento WAN a través de la implementación de DMVPN y gestiona las características de QoS para la WAN. El equipo router Cisco 3851 cumple funciones de enrutamiento, característica de traffic shaping para redes de la obra salesiana y la gestión del prototipo de IPv6.

Figura 15. Equipo Cisco ISR4451-X (Fuente; cisco.com)

Figura 16. Equipo Cisco 3851 (Fuente; cisco.com)

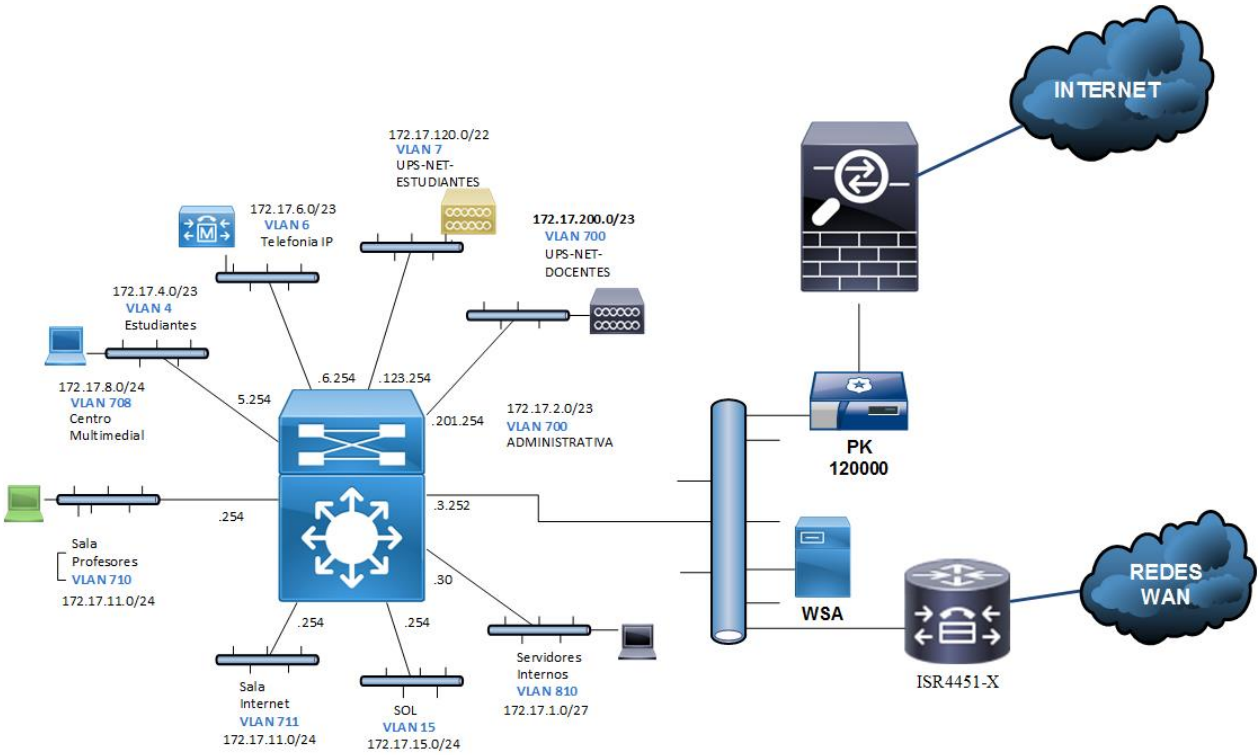


Figura 17, Diagrama lógico de frontera de red campus El Girón (Fuente; El autor)

3.2.Campus Sur.

El campus sur se encuentra ubicado en el sur de la ciudad de Quito en la calle Rumichaca y Av. Morán Valverde s/n en coordenadas aproximadas de latitud -0° 16´ 55,59”, longitud -78° 32´ 59,24” y altitud 2895m.

Para la identificación del rol que desempeñan los equipos y visibilizar la infraestructura de red en todos sus componentes utilizaremos el modelo jerárquico empresarial. Todos los campus de la UPS sede Quito tienen la misma infraestructura tecnológica por lo que se podrá visibilizar las misma organización, configuraciones comunes y conjunto de dispositivos.

3.2.1. Red de campus.

La infraestructura de red del campus Sur tiene la configuración de núcleo colapsado con un equipo Cisco Catalyst WS-C6506-E que tiene características redundantes únicamente en fuentes

de poder (WS-CAC-4000W-US), dispone de una supervisora (VS-SUP2T-10G), de una tarjeta de 48 SFP 1G (WS-X6848-SFP) y una tarjeta de 48 UTP 10/100/1000 (WS-X6848-GE-TX).

Tabla 8.

Componentes equipo Cisco catalyst WS-C6506-E (Fuente; El Autor)

NOMBRE COMPONENTE	DESCRIPCIÓN COMPONENTE	NÚMERO DE SERIE (SN)
WS-C6506-E	"Cisco Systems Inc. Catalyst 6500 6-slot Chassis System"	SN: SAL1646SD1M
WS-X6848-SFP	DESCR: "WS-X6848-SFP CEF720 48 port 1000mb SFP Rev. 3.0"	SN: SAL1938PA7A
WS-X6848-GE-TX	DESCR: "WS-X6848-GE-TX CEF720 48 port 10/100/1000mb Ethernet Rev. 1.0"	SN: SAL1703WV5B
VS-SUP2T-10G	DESCR: "VS-SUP2T-10G 5 ports Supervisor Engine 2T 10GE w/ CTS Rev. 1.4"	SN: SAL1702WHN9
WS-CAC-4000W-US"	DESCR: "220v AC power supply 4000 watt 1"	SN: SNI1645BL5A
WS-CAC-4000W-US"	DESCR: "220v AC power supply 4000 watt 1"	SN: SNI1645BL3G

El equipo WS-C6506-E es el equipo principal de la red y se encuentra toda la configuración de redes de área local virtuales (VLAN), servidor VLAN Trunking Protocol (VTP), enrutamiento, seguridad en la distribución con listas de control de acceso (ACL) y (QoS).

Tabla 9.

VLAN en el campus Sur de la UPS (Fuente; El autor)

VLAN	NOMBRE
1	DEFAULT
2	DMZ
3	ADMINISTRATIVA
4	CECASIS-EST-V1
5	CISCO
6	SUN
7	EVENTOSV2
8	SALA-BIBLIOTECA
10	WIRELESS-ESTUDIANTES
11	IPT

12	SALA-CECASIS
13	VLAN-VIDEO
14	VLAN-HP
15	ELECTRONICA
16	ISP
17	WLAN-IPCAM-CECASIS
18	WLAN-IPCAM-ELECTRONICA
19	INVESTIGACION
20	INTERNET-LOCAL
21	CIMA-SRV
22	RUI
23	INT-AVA
24	WLC-SUR
25	CAMARAS-IP-UIOS
26	EVENTOS
27	LAB-FISICA-UIO
28	CECASIS-EST-V2
29	SISTEMA_TV
30	DOCENTES-TIEMP-COMP
31	EUDOROAM
32	INSIDE-NUEVA
33	WSA-MNG
34	PORTAL
35	DATOS
36	EXPO
37	INVITADO
38	CONGRESO
39	STREAMING
40	ARUBA
41	COWORKING
42	ELECTRICA
43	MECANICA
48	WIRELESS-DOCENTES
138	CAMARAS-APS
148	LTC
149	RED-AVANZADA
150	ADM-WIRELESSV2

Tabla 10. *Direcciones IPv4 en las interfaces del equipo WS-C6506-E (Fuente; El autor)*

VLAN	**IP-ADDRESS**	**STATUS**
VLAN1	172.17.32.1	UP
VLAN2	172.17.33.254	UP
VLAN3	172.17.34.254	UP
VLAN4	172.17.37.253	UP
VLAN5	172.17.39.254	UP
VLAN7	172.17.130.254	UP
VLAN8	172.17.41.126	UP
VLAN10	172.17.215.254	UP
VLAN11	172.17.45.254	UP
VLAN12	172.17.41.190	UP
VLAN13	172.17.41.254	UP
VLAN16	172.17.16.254	UP
VLAN18	172.17.128.126	UP
VLAN19	172.17.128.62	UP
VLAN20	172.17.128.190	UP
VLAN21	172.17.128.254	UP
VLAN22	172.17.129.254	UP
VLAN23	172.17.132.254	UP
VLAN24	172.17.133.254	UP
VLAN25	172.17.134.126	UP
VLAN26	172.17.135.254	UP
VLAN27	UNASSIGNED	UP
VLAN28	172.17.136.254	UP
VLAN29	172.17.140.254	UP
VLAN30	172.17.143.254	UP
VLAN31	172.17.145.254	UP
VLAN32	172.17.146.254	UP
VLAN33	172.17.147.254	UP
VLAN40	172.17.240.254	UP
VLAN41	172.17.150.254	UP
VLAN42	172.17.242.254	UP
VLAN48	172.17.49.254	UP
VLAN112	UNASSIGNED	DOWN
VLAN138	172.17.139.254	UP
VLAN149	172.17.149.62	UP
VLAN150	UNASSIGNED	UP

Los equipos que se encuentran en la capa de acceso configurados con funciones únicamente de capa 2 son los modelos de las familias de Cisco catalyst 3750, 3750v2 y 2960(S/X) distribuidos por los diferentes cuartos intermediarios y secundarios de cableado estructurado (IDF/SDF). En estos equipos encontramos configuraciones de características de apilamiento de switch (stack), VTP, agregación de links (Ether-Channel), energía a través de ethernet (PoE) y características de QoS.

Figura 18. Equipo Cisco catalyst 3750/3750v2 (Fuente; cisco.com)

Figura 19. Equipo Cisco catalyst 2960(S/X) (Fuente; cisco.com)

El cableado estructurado del campus Sur está compuesto por cable UTP en cableado horizontal de categoría 6, 6A y 7A y cableado vertical en fibra óptica, los cuartos intermediarios y secundarios se conectan con cableado estructurado vertical al cuarto principal donde se tiene categoría 6 para el cableado horizontal en el centro de procesamiento de datos del campus.

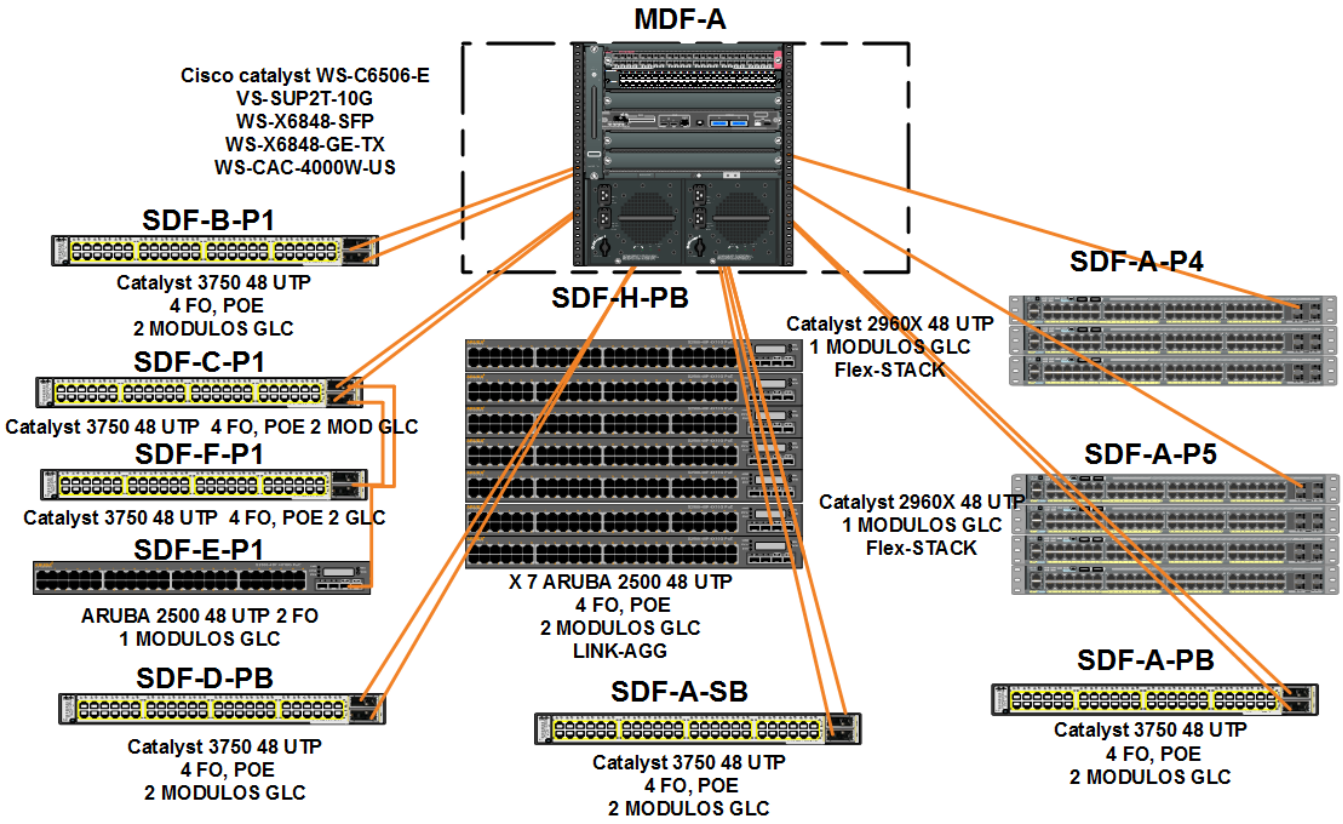


Figura 20. Distribución física de equipos campus Sur (Fuente; El autor)

Tabla 11.

Plataformas conectadas en la red de campus Sur (Fuente; El autor)

DISPOSITIVOS	PLATAFORMA
SW-IDF-RUI	WS-C2960S
SDF-A-PB	WS-C2960S
SDF-A-PB	WS-C2960S
SWCOREBCKP	WS-C3750G
SDF-BLOQUE-C	WS-C3750-
UPSS-IA	2811
UPSS-IA	2811
UPSUIOS-BKP	2851
UPSUIOS-BKP	2851
SW-OFIC	WS-C2960X
RT-BCKP-UIOV2	2851
RT-BCKP-UIOV2	2851
SDF-BB-P1-2	WS-C3750-
CISCO-LAB	WS-C2960X
CISCO-LAB	WS-C2960X
SDF-BB-PB	WS-C2960S
IDF-SW-5P-CECASIS	WS-C2960X
SDF-BA-BIBL	WS-C3750V
UPS-SUR.UIO.UPS.EDU.EC	ISR4331/K

IDF-BG-PB	WS-C3750G
IDF-BG-PB	WS-C3750G
WLC-UPSS	AIR-CT551
WLC-UPSS	AIR-CT551
UPS_NET.UPS.EDU.EC	2801

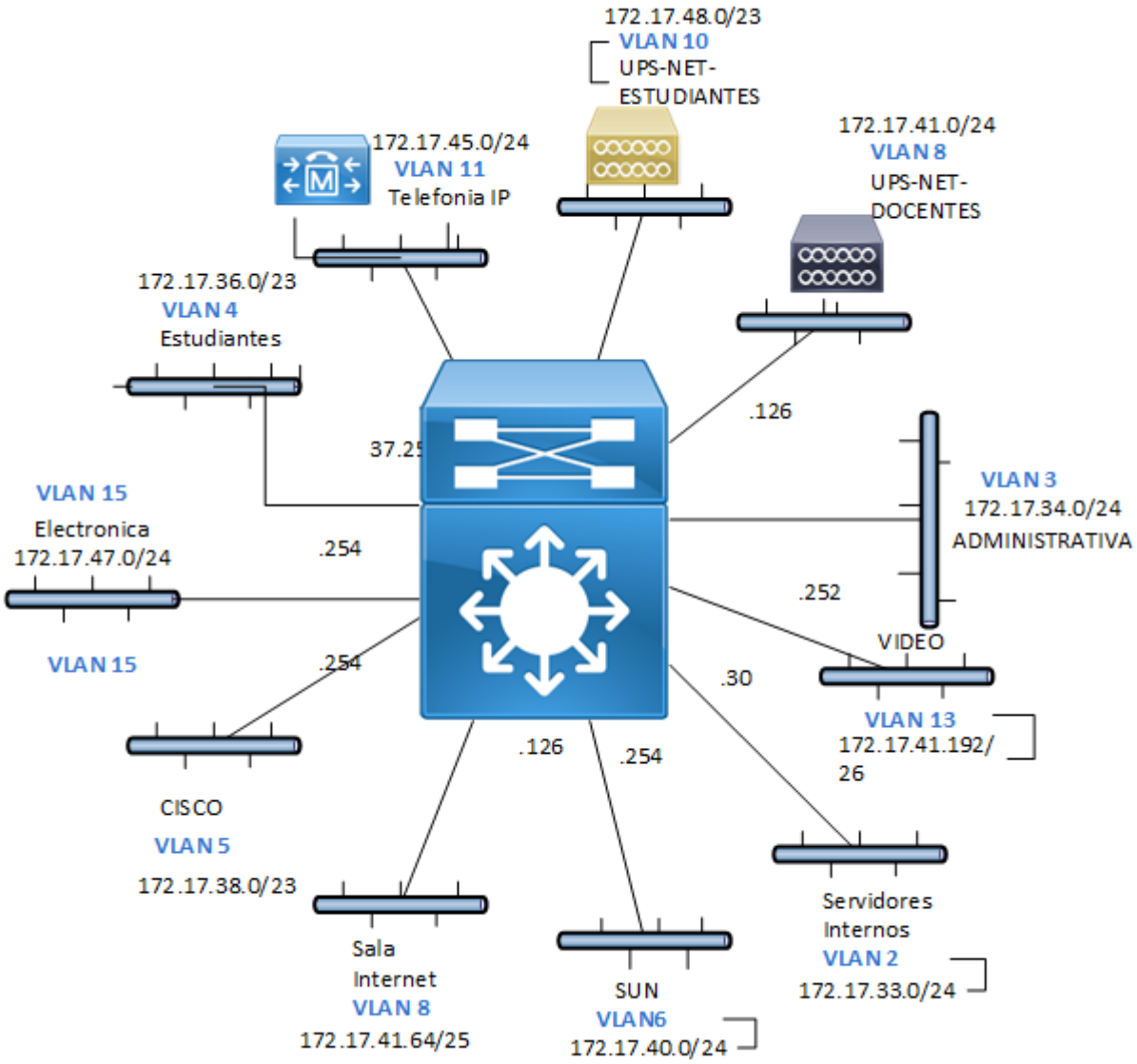


Figura 21, Diagrama lógico red campus Sur (Fuente; El autor)

Tabla 12,
Redes IPv4 campus Sur (Fuente; El autor)

VLAN	NOMBRE	RED IPV4
1	DEFAULT	172.17.32.0/24
2	DMZ	172.17.33.0/24
3	ADMINISTRATIVA	172.17.34.0/24
4	CECASIS-EST-V1	172.17.36.0/23
5	CISCO	172.17.38.0/25
6	SUN	172.17.40.0/24
7	EVENTOSV2	172.17.130.0/24
8	SALA-BIBLIOTECA	172.17.41.64/26
10	WIRELESS-ESTUDIANTES	172.17.208.0/29
11	IPT	172.17.45.0/24
12	SALA-CECASIS	172.17.41.129/26
13	VLAN-VIDEO	172.17.41.193/26
14	VLAN-HP	172.17.42.0/24
15	ELECTRONICA	172.17.47.0/24
16	ISP	172.17.16.0/24
17	WLAN-IPCAM-CECASIS	NA
18	WLAN-IPCAM-ELECTRONICA	172.17.128.64/26
19	INVESTIGACION	172.17.128.0/26
20	INTERNET-LOCAL	172.17.129.0/26
21	CIMA-SRV	172.17.128.192/26
22	RUI	172.17.129.0/24
23	INT-AVA	172.17.132.0/24
24	WLC-SUR	172.17.133.0/24
25	CAMARAS-IP-UIOS	172.17.134.0/25
26	EVENTOS	172.17.135.0/24
27	LAB-FISICA-UIO	172.17.136.0/25
28	CECASIS-EST-V2	172.17.136.129/25
29	SISTEMA_TV	172.17.140.0/24
30	DOCENTES-TIEMP-COMP	172.17.142.0/23
31	EUDOROAM	172.17.144.0/23
32	INSIDE-NUEVA	172.17.146.0/24
33	WSA-MNG	172.17.147.0/24
34	PORTAL	NA
35	DATOS	NA
36	EXPO	NA
37	INVITADO	NA
38	CONGRESO	NA
39	STREAMING	NA
40	ARUBA	172.17.240.0/24
41	COWORKING	172.17.150.0/24
42	ELECTRICA	172.17.242.0/24
43	MECANICA	172.17.151.0/24
48	WIRELESS-DOCENTES	172.17.48.0/23

138	CAMARAS-APS	172.17.138.0/23
148	LTC	172.17.148.0/24
149	RED-AVANZADA	172.17.149.0/26
150	ADM-WIRELESSV2	172.17.35.0/24

3.2.2. Red de frontera.

La red de frontera del campus Sur está compuesta por toda la infraestructura de conexión con los recursos externos, describiremos la protección de conexión a internet, acceso remoto VPN y WAN.

3.2.2.1. Conexión de Internet

En esta área funcional se gestiona el acceso a internet y la infraestructura de frontera que permite una navegación segura y controlada. Entre el conjunto de equipos que son pate de la frontera de la red, está un equipo firewall adaptivo de seguridad de siguiente generación (NGFW) Cisco ASA 5515, encargado de la gestión y administración del aseguramiento de navegación hacia el internet con un complemento de servicio de firePOWER que potencia la robustez de la solución con IPS y protección avanzada contra amenazas.

Figura 22. Equipo Cisco NGFW ASA 5515 (Fuente; cisco.com)

La gestión del filtrado de navegación web está a cargo del dispositivo de seguridad web de Cisco Web Security Appliance (WSA) S380, este equipo mantiene la estructura tradicional de filtrado web complementarias con características de reputación de sitios web, y un análisis de monitoreo en tiempo real para mitigar problemas de seguridad de la red.

Figura 23. Equipo Cisco WSA S380 (Fuente; cisco.com)

La gestión del ancho de banda y calidad de servicio QoS de internet se realiza a través del equipo de marca Blue Coat PacketShaper 12000 que realiza inspección de paquetes en profundidad a la entrada y salida del tráfico, permitiendo tener una gran visibilidad del consumo de las aplicaciones que usan el servicio de internet.

Figura 24. Equipo Blue Coat PacketShaper 12000 (Fuente; bluecoat.com)

3.2.2.2. Acceso remoto y VPN

En esta área funcional encontramos al equipo Cisco NGFW ASA 5545 con el que gestionamos la posibilidad de conexiones seguras a través de medios públicos como el internet, el NGFW se convierte en un concentrador de VPN facilitando el ingreso externo seguro a los recursos de red disponibles.

3.2.2.3. WAN

Para la conexión del campus con las redes de área extendida utilizamos equipos enrutadores de dos tipos, el equipo Cisco ISR4331 es el router principal que cumple funciones de gateway de voz, tiene las configuraciones de gestión de enrutamiento WAN a través de la implementación de DMVPN y gestiona las características de QoS para la WAN. El equipo router Cisco 2851 cumple funciones de enrutamiento, característica de traffic shaping para redes de laboratorios.

Figura 25. Equipo Cisco ISR4331 (Fuente; cisco.com)

Figura 26, Equipo Cisco 2851 (Fuente; cisco.com)

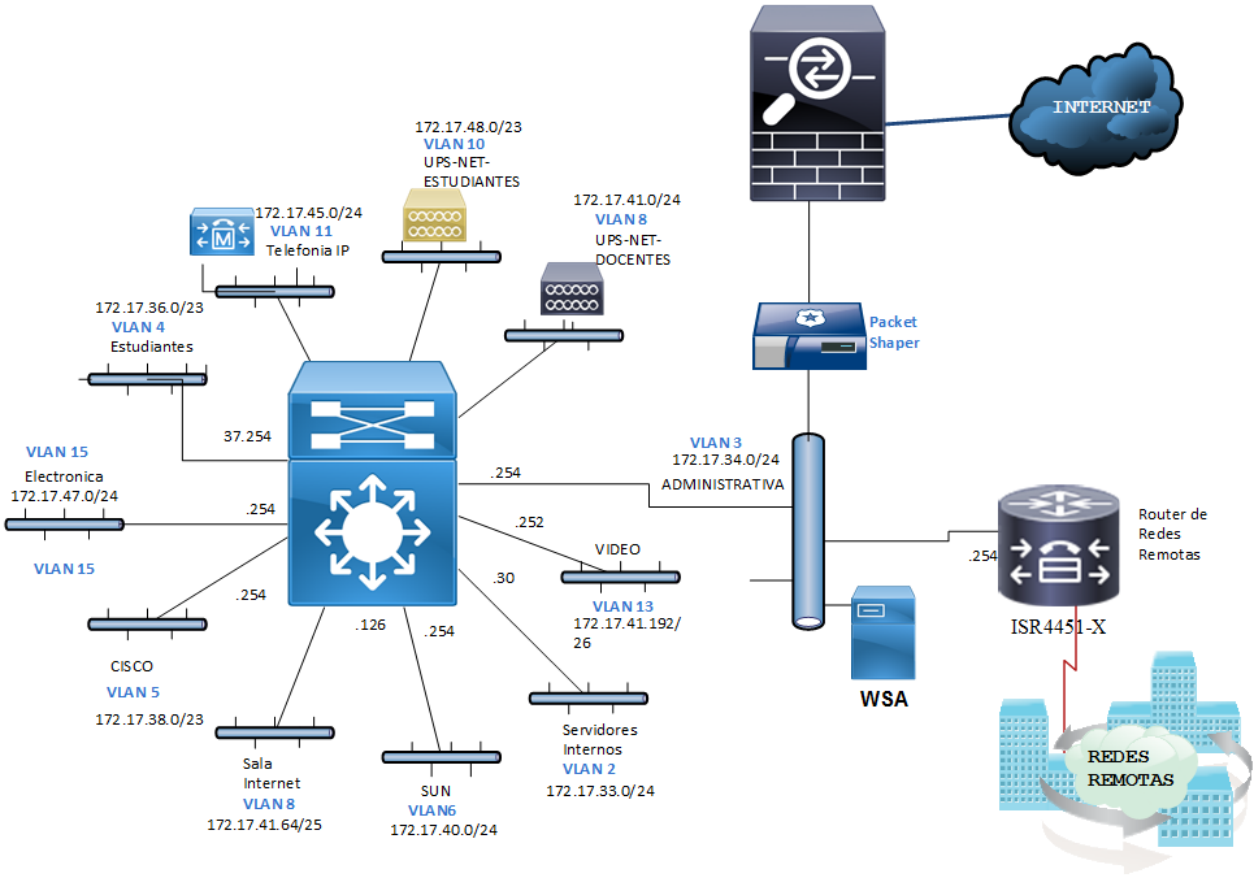


Figura 27, Diagrama lógico de frontera de la empresa campus Sur (Fuente; El autor)

3.3.Campus Kennedy.

El campus Kennedy está ubicado en el norte de la ciudad de Quito en la calle Rafael Bustamante SN funciona junto al colegio técnico salesiano Don Bosco en coordenadas de latitud -0° 8'35.46", longitud -78°28'43.65" y altitud 2820m.

El modelamiento que se utilizara para el establecimiento de la línea base de la red es modelo jerárquico empresarial que permite obtener identificación de las relaciones entre dispositivos y la interacción entre los componentes de la red de campus.

3.3.1. Red de campus.

El campus Kennedy está compuesto por un modelo colapsado distribución/núcleo con un equipo Cisco Catalyst 4507R con una infraestructura redundante a nivel de supervisora (WS-X4515) y fuentes de poder (PWR-C45-1400AC), tiene una tarjeta 48 UTP 1G(WS-X4548-GB-RJ45V), dos tarjetas 24 UTP de (WS-X4424-GB-RJ45) y una tarjeta 48 SFP 1G (WS-X4448-GB-SFP)

Este equipo es la base fundamental de la infraestructura de la red de campus que se encarga de la administración del tráfico, aplicación de políticas de QoS, enrutamiento, VLAN y demás funcionalidades convencionales de los equipos de núcleo en la red de campus.

Figura 28, Equipo Cisco Catalyst 4507R (Fuente; El autor)

Tabla 13.
Componentes Equipo Cisco catalyst WS-C4507R (Fuente; El autor)

NOMBRE COMPONENTE	DESCRIPCIÓN COMPONENTE	NÚMERO DE SERIE (SN)
WS-C4507R	"Cisco Systems Inc. WS-C4507R 7 slot switch "	SN: FOX104000RL
WS-X4515	"Supervisor IV with 2 1000BaseX GBIC ports"	SN: JAE1038BSMP
WS-X4515	"Supervisor IV with 2 1000BaseX GBIC ports"	SN: JAE1040CUS9
WS-X4448-GB-SFP	"1000BaseX (SFP) with 48 SFP ports"	SN: JAE1047FTS5
WS-X4424-GB-RJ45	"10/100/1000BaseT (RJ45) with 48 10/100/1000 baseT ports"	SN: JAE1037BFJP
WS-X4424-GB-RJ45	"10/100/1000BaseT (RJ45) with 48 10/100/1000 baseT ports"	SN: JAE1126NECS
WS-X4548-GB-RJ45V	"10/100/1000BaseT (RJ45)V with 48 10/100/1000 baseT voice power ports (Cisco/IEE"	SN: JAE12021CY5
PWR-C45-1400AC	"Power Supply (AC 1400W)"	SN: DTH10187271
PWR-C45-1400AC	"Power Supply (AC 1400W)"	SN: DTH10187272

El equipo WS-C4507-R es el equipo principal de la red y se encuentra toda la configuración de redes de área local virtuales (VLAN), servidor VTP, enrutamiento, seguridad en la distribución con ACL y políticas de QoS.

Tabla 14.
VLAN en el campus Kennedy de la UPS (Fuente; El autor)

VLAN	NOMBRE
1	DEFAULT
2	LAN_DMZ
3	ADM
4	LABS-ESTUDIANTES
7	TELEFONIA_IP
8	SALA_BIBLIOTECA
9	SALA_PROFESORES
10	WLAN_ESTUDIANTES
11	VIDEO-CONFERENCIA
12	LAN_SERVIDORES_INTERNOS
13	INTERNET-TELCO
14	LAN_ELECTRICA
18	LAN_INVESTIGACION
19	LAN_WLC
20	VLAN-DOCENTES
21	LABORATORIO_WLAN
22	VLAN-COLEGIO-WLAN
30	WSA
31	PRODUCCION-WSA
224	CES-DOCENTES
226	CES-COLEGIO
228	CES-ESCUELA
229	CES-ADM
230	CES-SERVER
231	WLC-UNIFI
232	EVENTOS
234	CES-DOCENTE234

Tabla 15.
Direcciones IPv4 en las interfaces del equipo WS-4507-R (Fuente; El autor)

VLAN	IP-ADDRESS	STATUS
VLAN1	172.17.16.1	UP
VLAN2	172.17.17.254	UP
VLAN3	172.17.18.254	UP
VLAN4	172.17.20.254	UP
VLAN7	172.17.23.254	UP
VLAN8	172.17.21.62	UP
VLAN9	172.17.21.126	UP
VLAN10	172.17.27.254	UP
VLAN11	172.17.21.254	UP
VLAN12	172.17.24.62	UP
VLAN13	UNASSIGNED	UP
VLAN14	172.17.25.254	UP
VLAN18	172.17.28.62	UP
VLAN19	172.17.144.254	UP
VLAN20	172.17.29.254	UP
VLAN21	172.17.145.254	UP
VLAN30	172.17.30.30	UP
VLAN224	172.17.224.254	UP
VLAN228	172.17.228.254	UP
VLAN229	172.17.229.254	UP
VLAN231	172.17.231.254	UP
VLAN232	172.17.232.254	UP
VLAN234	172.17.235.254	UP

Los equipos encargados de la función de acceso capa L2 son equipos de las familias Cisco Catalyst 3750, 2960 y equipos de marca 3COM que están distribuidos en los diferentes cuartos de comunicaciones del campus. En estos equipos localizamos configuraciones de stack, VTP, agregación de links, PoE y características de QoS.

Figura 29. Equipo Cisco catalyst 3750/3750v2 (Fuente; cisco.com)

Figura 30. Equipo Cisco catalyst 2960(S/X) (Fuente; cisco.com)

El cableado estructurado del campus Kennedy está compuesto por cable UTP en cableado horizontal de categoría 6 y cableado vertical en fibra óptica, los cuartos intermediarios y secundarios se conectan con cableado estructurado vertical al cuarto principal donde se tiene categoría 6A para el cableado horizontal en el centro de procesamiento de datos del campus.

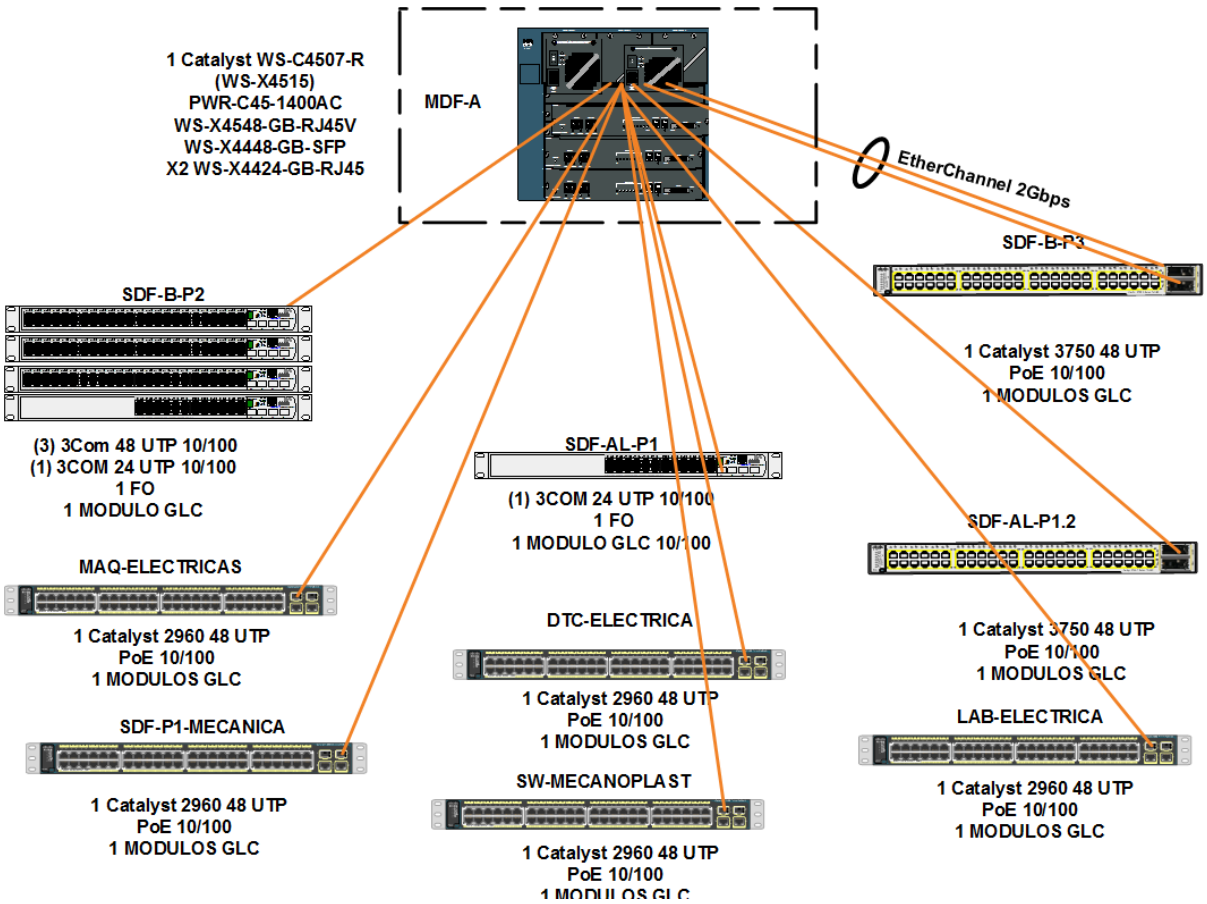


Figura 31, Distribución física de equipos campus Sur (Fuente; El autor)

Tabla 16.
Plataformas conectadas en la red de campus Kennedy (Fuente; El autor)

DISPOSITIVO	PLATAFORMA
APTEATRO	LINUX
CN3AB013TP	V-M200
CN35B0123S	V-M200
LAB-ELECTRICA	WS-C2960-4GIG
AP-LAB-ELECTRONICA1	AIR-LAP125GIG
DTC-ELECTRICA	WS-C2960-4GIG
SDF-P1-MECANICA	WS-C2960-2GIG
WLCUIOK	AIR-CT2504GIG
WLCUIOK	AIR-CT2504GIG
MICROBOTICA	WS-C2960-4GIG
UPS-KENNEDY.UIO.UPS.EDU.EC	ISR4331/K9GIG
AP_CTDB	AIR-LAP113FAS
MAQ-ELECTRICAS	WS-C2960-4GIG
CN35B010TJ	V-M200
2PLABORATORIOS	LINUX
SDF-B-P3	WS-C3750-4GIG
SDF-B-P3	WS-C3750-4GIG
CN35B010BN	V-M200
SW-MECANOPLAST	WS-C2960X-GIG

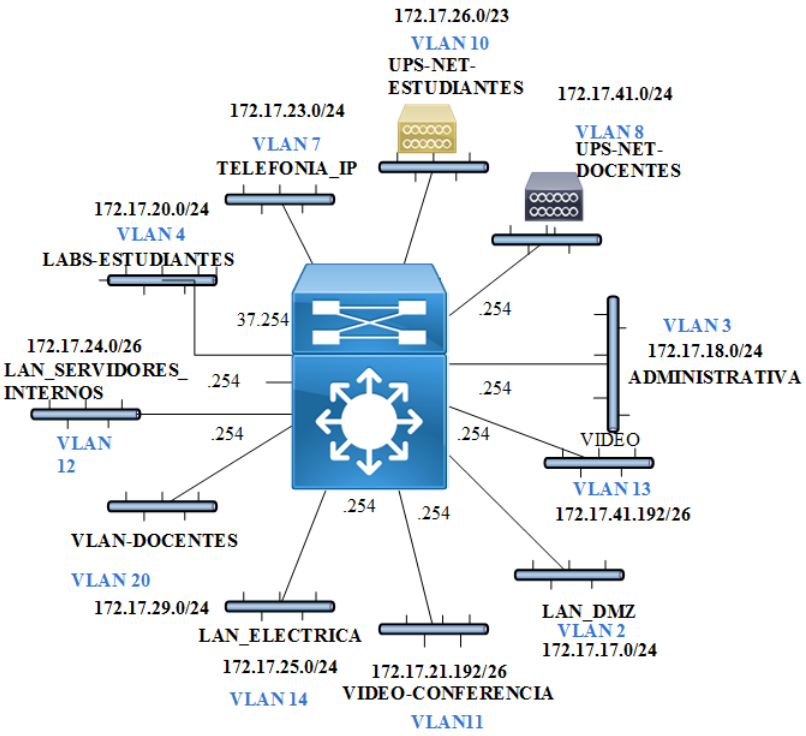


Figura 32. Diagrama lógico de frontera de la empresa campus Kennedy (Fuente; El autor)

Tabla 17. *Redes IPv4 campus Kennedy*

(Fuente; El autor)

VLAN	NOMBRE	RED IPV4
1	DEFAULT	172.17.16.0/24
2	LAN_DMZ	172.17.17.0/24
3	ADM	172.17.18.0/24
4	LABS-ESTUDIANTES	172.17.20.0/24
7	TELEFONIA_IP	172.17.23.0/24
8	SALA_BIBLIOTECA	NA
9	SALA_PROFESORES	172.17.21.64/26
10	WLAN_ESTUDIANTES	172.17.26.0/23
11	VIDEO-CONFERENCIA	172.17.21.192/26
12	LAN_SERVIDORES_INTERNOS	172.17.24.0/26
13	INTERNET-TELCO	NA
14	LAN_ELECTRICA	172.17.25.0/24
18	LAN_INVESTIGACION	172.17.28.0/26
19	LAN_WLC	172.17.144.0/24
20	VLAN-DOCENTES	172.17.29.0/24
21	LABORATORIO_WLAN	172.17.145.0/24
22	VLAN-COLEGIO-WLAN	NA
30	WSA	172.17.30.0/27
31	PRODUCCION-WSA	NA
224	CES-DOCENTES	172.17.224.0/23
226	CES-COLEGIO	NA
228	CES-ESCUELA	172.17.228.0/24
229	CES-ADM	172.17.229.0/24
230	CES-SERVER	NA
231	WLC-UNIFI	172.17.231.0/24
232	EVENTOS	172.17.232.0/24
234	CES-DOCENTE234	172.17.234.0/23

3.3.2. Red de frontera.

La red de frontera del campus Kennedy está compuesta por toda la infraestructura de conexión con los recursos externos, describiremos la protección de conexión a internet, acceso remoto VPN y WAN.

3.3.2.1. Conexión de Internet

En esta área se gestiona el acceso a internet y la infraestructura que permite una navegación segura y controlada. El conjunto de equipos que son pate de la frontera de la red, está un equipo firewall adaptivo de seguridad de siguiente generación (NGFW) Cisco ASA 5512, encargado de la gestión y administración del aseguramiento de navegación hacia el internet con un complemento de servicio de firePOWER que potencia la robustez de la solución con IPS y protección avanzada contra amenazas.

Figura 33. Equipo Cisco NGFW ASA 5512 (Fuente; cisco.com)

La gestión del filtrado de navegación web está a cargo del dispositivo de seguridad web de Cisco Web Security Appliance (WSA) S170, este equipo mantiene la estructura tradicional de filtrado web complementarias con características de reputación de sitios web, y un análisis de monitoreo en tiempo real para mitigar problemas de seguridad de la red.

Figura 34. Equipo Cisco WSA S170 (Fuente; cisco.com)

La gestión del ancho de banda y calidad de servicio QoS de internet se realiza a través del equipo de marca Blue Coat PacketShaper 12000 que realiza inspección de paquetes en

profundidad a la entrada y salida del tráfico, permitiendo tener una gran visibilidad del consumo de las aplicaciones que usan el servicio de internet.

Figura 35. Equipo Blue Coat PacketShaper 12000 (Fuente; bluecoat.com)

3.3.2.2. Acceso remoto y VPN

En esta área funcional encontramos al equipo Cisco NGFW ASA 5512 con el que gestionamos la posibilidad de conexiones seguras a través de medios públicos como el internet, el NGFW se convierte en un concentrador de VPN facilitando el ingreso externo seguro a los recursos de red disponibles.

3.3.2.3. WAN

para la conexión del campus con las redes de área extendida utilizamos equipos enrutadores de dos tipos, el equipo Cisco ISR4331 es el router principal que cumple funciones de gateway de voz, tiene las configuraciones de gestión de enrutamiento WAN a través de la implementación de DMVPN y gestiona las características de QoS para la WAN. El equipo router Cisco 2851 cumple funciones de enrutamiento, característica de traffic shaping para redes de la red del colegio técnico Don Bosco.

Figura 36. Equipo Cisco ISR4331 (Fuente; cisco.com)

Figura 37, Equipo Cisco 2851 (Fuente; cisco.com)

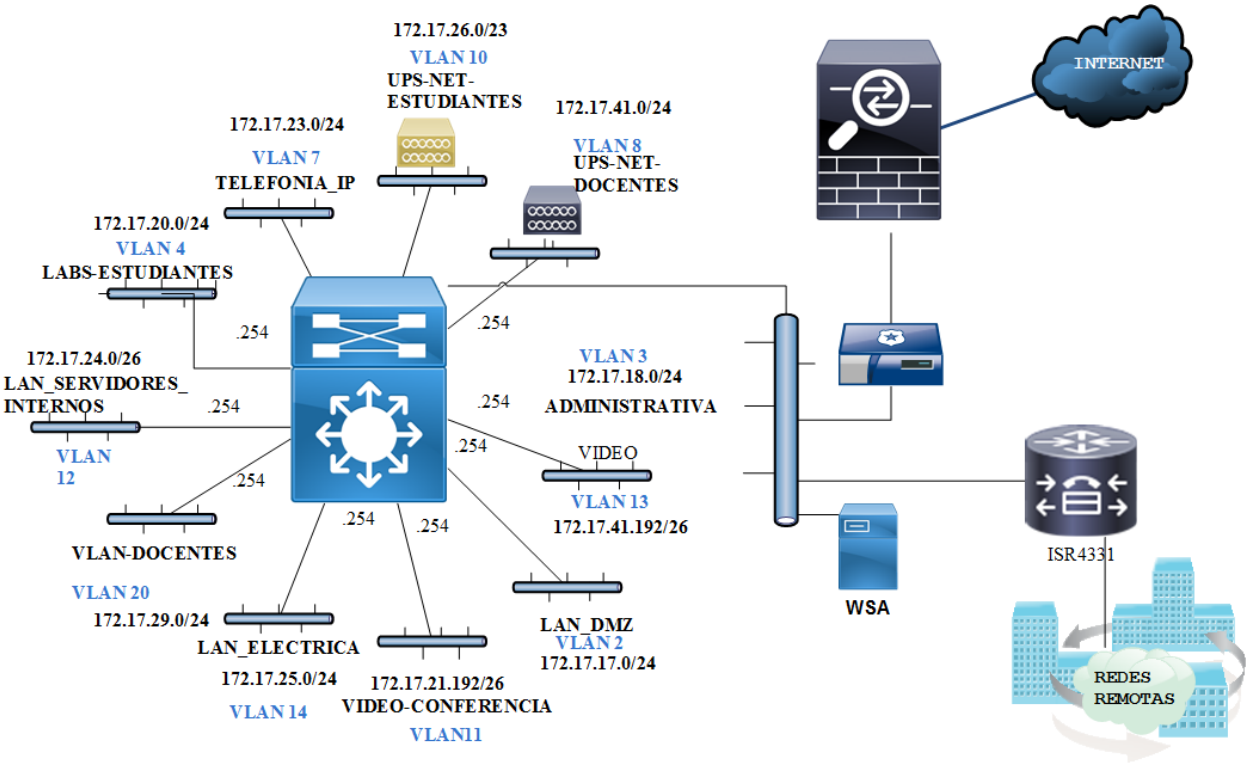


Figura 38. Diagrama lógico de frontera de la empresa campus Kennedy (Fuente, El autor)

CAPÍTULO 4: DISEÑO DE PLAN IPV6 E IMPLEMENTACIÓN DE PROTOTIPO

4.1.Diseño del plan IPv6.

Para el diseño del plan IPv6 se ha considerado el uso de las direcciones de tipo único global (unicast global), este direccionamiento nos permitirá el acceso a recursos IPv6 disponibles en internet.

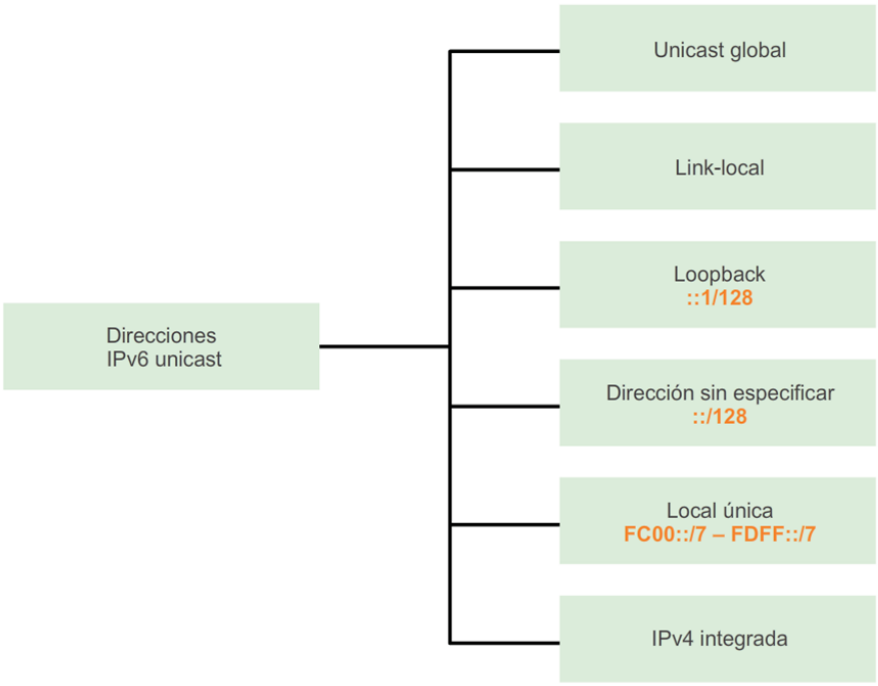


Figura 39. Direcciones IPv6 unicast (Fuente; Tomado de Cisco Network Academy)

Se ha solicitado al ISP CEDIA (Fundación Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado), la asignación de los segmentos IPv6 de red para los campus de la sede Quito.

La asignación recibida de CEDIA de redes IPv6 para la sede Quito es:

- Campus El Girón: 2800:68:22::/48
- Campus Kennedy: 2800:68:21::/48
- Campus Sur: 2800:68:16::/48

El criterio escogido para el diseño de la ejecución del plan IP será usar los 16 bit restantes de la dirección IPv6 del segmento de red /64 para la del direccionamiento y visibilizar la jerarquía del direccionamiento.

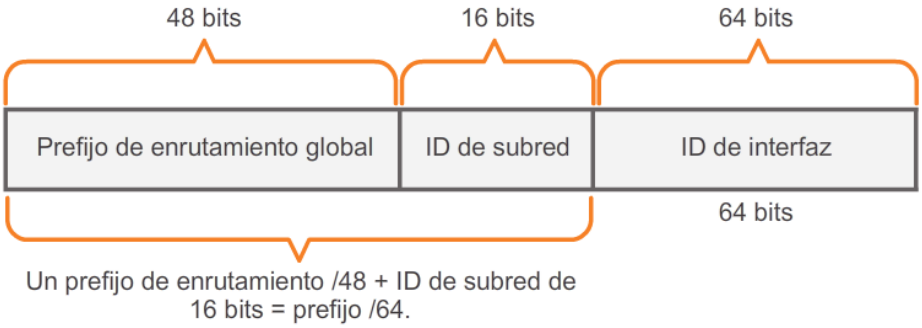


Figura 40. Estructura de IPv6 unicast global (Fuente; Tomada de Cisco Network Academy)

Direccionamiento asignado para el ejemplo: 2800:68:22::/48

En la dirección IPv6 completa encontramos 8 hextetos (un hexteto es una denominación no oficial a la equivalencia de 4 números hexadecimales) para la porción de red y 8 hextetos para la porción de host, cada hexteto tiene una denominación de “nibble” que representa una máscara de límite de 4 bits; la creación de subredes bajo el principio de nibble es más fácil de gestionar y de entender.

Ejemplo#1:

2800:0068:0022:***RRRR***:*HHHH:HHHH:HHHH:HHHH/64*

En la dirección IPv6 del ejemplo #1 encontramos las letras RRRR representando el hexteto /16 de red que nos permitirá crear subredes para la organización interna del direccionamiento.

Las letras HHHH representan los 8 hextetos para la porción de la interface de red de los dispositivos finales.

En la aplicación del diseño del plan IPv6 de direccionamiento se mostrará la jerarquía y la organización de la red dentro del direccionamiento.

Del prefijo asignado por CEDIA /48 es el prefijo global de enrutamiento para la UPS (campus Sur, El Girón y Kennedy). Nos resta los 16 bits descritos anteriormente en el ejemplo#1 con las letras RRRR para las subredes representados los hextetos en las posiciones /52 /56 /60 /64.

La posición /52 se ha escogido para crecimiento futuro y permanecerá en 0.

La posición /56 representara la primera jerarquía del direccionamiento que en el diseño está asignado a representar la unidad organizacional según la tabla #19 para el campus El Girón.

Tabla 18.

Unidad Organizacional e ID asignado en la posición /56 (Fuente; El autor)

ID	UNIDAD ORGANIZACIONAL
A	UPS
B	ABYAYALA
C	CSRFP
D	INSPECTORIA
E	ABD
F	LNS

En el caso del campus El Girón existen configuradas 45 VLAN las que podrían necesitar de direccionamiento para esto asignamos dos posiciones /60 y /64 que nos dan un soporte para $\mathbf{2^{8}}$ = 256 combinaciones o subredes.

Es muy importante que para la aplicación en una interface de cualquier dispositivo final siempre se asigne el prefijo /64 para que los procesos de auto configuración funcionen.

Ejemplo de aplicación del direccionamiento IPv6 con el uso de las consideraciones propuestas:

Caso de asignación de una dirección IPv6 para una subred por defecto, que deberá ser configurada en la SVI de VLAN 1 en el switch de núcleo de la UPS campus El Girón.

Dirección IPv6 /48 asignada a la UPS campus El Girón.

2800:0068:0022/48

Posición /52 asignado para reserva, en esta posición asignaremos un cero en hexadecimal "**0**".

Posición /56 debe reflejar la unidad organizacional, que en este caso es la UPS asignaremos el equivalente de la tabla # 19 asignada que es el número en hexadecimal "**A**".

Anteriormente se describió que para las redes en el campus se deberán usar las posiciones /60 y /64, como la necesidad a cubrir es la VLAN uno le corresponde la asignación del numero hexadecimal "**01**".

Por lo que la dirección IPv6 según la aplicación de la recomendación de diseño seria:

Dirección IPv6 completa

2800:0068:0022:***0A01***:0000:0000:0000:0001/64

Dirección IPv6 en formato simplificado (eliminar los ceros de la izquierda de cada hexteto).

2800:68:22:A01:0:0:0:1/64

Dirección IPv6 en formato comprimido (utilizar :: doble dos puntos para una cadena de ceros consecutivos pero una sola vez en la dirección).

2800:68:22:A01::1/64

Para la asignación del plan IPv6 se tomará la tabla 8 de direccionamiento IPv4 del campus El Girón y se asignará el equivalente de la aplicación de esta recomendación en la tabla 20.

Tabla 19.
Plan IPv6 campus El Girón (Fuente; El autor)

#	/48			/52	/56	/60	/64	IPv6 INT	VLAN ID	NOMBRE
	2800	68	22	0	0	0	0	::1		
1	2800	68	22	0	A	0	1	::1	1	DEFAULT
2	2800	68	22	0	A	0	2	::1	3	ADMINISTRATIVA
3	2800	68	22	0	A	0	3	::1	4	VLAN-RELOJ

4	2800	68	22	0	A	0	4	::1	6	IPT
5	2800	68	22	0	A	0	5	::1	7	UPS-NET-ESTUDIANTES
6	2800	68	22	0	A	0	6	::1	9	VLAN-SALA-INTERNET
7	2800	68	22	0	A	0	7	::1	10	VIDEO
8	2800	68	22	0	A	0	8	::1	11	INTERNET
9	2800	68	22	0	C	0	1	::1	12	CSRFP
10	2800	68	22	0	A	0	A	::1	13	SOL
11	2800	68	22	0	D	0	1	::1	14	INSPECTORIA-ADMINISTRATIVA
12	2800	68	22	0	E	0	1	::1	15	ADB
13	2800	68	22	0	B	0	1	::1	16	ABYA-YALA
14	2800	68	22	0	A	0	E	::1	17	CAMARA-IP
15	2800	68	22	0	F	0	1	::1	18	LNS
16	2800	68	22	0	A	1	1	::1	19	INTERNET-TVCABLE
17	2800	68	22	0	A	1	2	::1	20	VWLC
18	2800	68	22	0	A	1	3	::1	24	VLAN0024
19	2800	68	22	0	A	1	4	::1	30	PACKET
20	2800	68	22	0	A	1	5	::1	99	VLAN0099
21	2800	68	22	0	A	1	6	::1	100	EVENTOS
22	2800	68	22	0	A	1	7	::1	112	ADMINISTRATIVOSV2
23	2800	68	22	0	A	1	8	::1	114	VLAN-WLC
24	2800	68	22	0	A	1	9	::1	115	VLAN-WLC2
25	2800	68	22	0	A	1	A	::1	118	IDIOMAS
26	2800	68	22	0	A	1	B	::1	119	SRV-INTERNOS-V2
27	2800	68	22	0	A	1	C	::1	120	EVENTOSV2
28	2800	68	22	0	A	1	D	::1	125	ASA
29	2800	68	22	0	A	1	E	::1	126	ASA-BC
30	2800	68	22	0	A	1	F	::1	156	3CX
31	2800	68	22	0	A	2	1	::1	239	COWORKING
32	2800	68	22	0	A	2	2	::1	240	ESTUDIANTES-V2
33	2800	68	22	0	A	2	3	::1	500	CSRFPV2
34	2800	68	22	0	A	2	4	::1	700	DOCENTES/23
35	2800	68	22	0	A	2	5	::1	704	CECASIG
36	2800	68	22	0	A	2	6	::1	708	CENTRO-MULTIMEDIAL
37	2800	68	22	0	A	2	7	::1	710	DOCENTES

38	2800	68	22	0	A	2	8	::1	711	SALA-INTERNET
39	2800	68	22	0	A	2	9	::1	810	SERVIDORES-INTERNOS
40	2800	68	22	0	A	2	A	::1	820	SERVIDORES-PUBLICOS
41	2800	68	22	0	A	2	B	::1	830	SERVIDORES-PROXY
42	2800	68	22	0	A	2	C	::1	840	PROXIM
43	2800	68	22	0	A	2	D	::1	99	TELCONET

Para el plan IPv6 del campus Sur se mantiene la misma planificación y criterios aplicados en la explicación de cómo fue diseñado el plan IPv6, la modificación para este campus está en el prefijo asignado por CEDIA, la existencia de 47 VLAN y la tabla 21 que muestra las unidades organizacionales.

Tabla 20.

Unidad Organizacional e ID asignado en la posición /56 (Fuente; El autor)

ID	UNIDAD ORGANIZACIONAL
A	UPS
B	RESIDENCIA
C	COWORKING
D	EDUROAM
E	EVENTOS

Tabla 21.

Plan IPv6 Campus Sur (Fuente; El autor)

#	/48			/52	/56	/60	/64	IPV6 INT	VLAN ID	NOMBRE
	2800	68	16	0	0	0	0	0:0:0:1		
1	2800	68	16	0	A	0	1	::1	1	DEFAULT
2	2800	68	16	0	A	0	2	::1	2	DMZ
3	2800	68	16	0	A	0	3	::1	3	ADMINISTRATIVA
4	2800	68	16	0	A	0	4	::1	4	CECASIS-EST-V1
5	2800	68	16	0	A	0	5	::1	5	CISCO
6	2800	68	16	0	A	0	6	::1	6	SUN
7	2800	68	16	0	A	0	7	::1	7	EVENTOSV2
8	2800	68	16	0	A	0	8	::1	8	SALA-BIBLIOTECA

9	2800	68	16	0	A	0	9	::1	10	WIRELESS-ESTUDIANTES
10	2800	68	16	0	A	0	A	::1	11	IPT
11	2800	68	16	0	A	0	B	::1	12	SALA-CECASIS
12	2800	68	16	0	A	0	C	::1	13	VLAN-VIDEO
13	2800	68	16	0	A	0	D	::1	14	VLAN-HP
14	2800	68	16	0	A	0	E	::1	15	ELECTRONICA
15	2800	68	16	0	A	0	F	::1	16	ISP
16	2800	68	16	0	A	1	1	::1	17	WLAN-IPCAM-CECASIS
17	2800	68	16	0	A	1	2	::1	18	WLAN-IPCAM-ELECTRONICA
18	2800	68	16	0	A	1	3	::1	19	INVESTIGACION
19	2800	68	16	0	A	1	4	::1	20	INTERNET-LOCAL
20	2800	68	16	0	A	1	5	::1	21	CIMA-SRV
21	2800	68	16	0	B	0	1	::1	22	RUI
22	2800	68	16	0	A	1	7	::1	23	INT-AVA
23	2800	68	16	0	A	1	8	::1	24	WLC-SUR
24	2800	68	16	0	A	1	9	::1	25	CAMARAS-IP-UIOS
25	2800	68	16	0	A	1	A	::1	26	EVENTOS
26	2800	68	16	0	A	1	B	::1	27	LAB-FISICA-UIO
27	2800	68	16	0	A	1	C	::1	28	CECASIS-EST-V2
28	2800	68	16	0	A	1	D	::1	29	SISTEMA_TV
29	2800	68	16	0	A	1	E	::1	30	DOCENTES-TIEMP-COMP
30	2800	68	16	0	A	1	F	::1	31	EUDOROAM
31	2800	68	16	0	A	2	1	::1	32	INSIDE-NUEVA
32	2800	68	16	0	A	2	2	::1	33	WSA-MNG
33	2800	68	16	0	A	2	3	::1	34	PORTAL
34	2800	68	16	0	A	2	4	::1	35	DATOS
35	2800	68	16	0	E	0	1	::1	36	EXPO
36	2800	68	16	0	E	0	2	::1	37	INVITADO
37	2800	68	16	0	E	0	3	::1	38	CONGRESO
38	2800	68	16	0	E	0	4	::1	39	STREAMING
39	2800	68	16	0	A	2	9	::1	40	ARUBA
40	2800	68	16	0	C	0	1	::1	41	COWORKING
41	2800	68	16	0	A	2	B	::1	42	ELECTRICA
42	2800	68	16	0	A	2	C	::1	43	MECANICA
43	2800	68	16	0	A	2	D	::1	48	WIRELESS-DOCENTES
44	2800	68	16	0	A	2	E	::1	138	CAMARAS-APS
45	2800	68	16	0	A	2	F	::1	148	LTC
46	2800	68	16	0	A	3	1	::1	149	RED-AVANZADA
47	2800	68	16	0	A	3	2	::1	150	ADM-WIRELESSV2

Para el campus Kennedy el direccionamiento IPv6 mantiene lo mismos lineamientos de diseño, tenemos la existencia de 27 VLAN, cambia el prefijo asignado por CEDIA y la tabla que muestra las unidades organizacionales del campus.

Tabla 22.
Unidad Organizacional e ID asignado en la posición /56 (Fuente; El autor)

ID	UNIDAD ORGANIZACIONAL
A	UPS
B	CES
C	IMPRENTA
D	MECANOPLAS

Tabla 23.
Plan IP campus Kennedy (Fuente; El Autor)

#	/48			/52	/56	/60	/64	IPv6 INT	VLAN ID	NOMBRE
	2800	68	21	0	0	0	0	0:0:0:1		
1	2800	68	21	0	A	0	1	::1	1	default
2	2800	68	21	0	A	0	2	::1	2	LAN_DMZ
3	2800	68	21	0	A	0	3	::1	3	ADM
4	2800	68	21	0	A	0	4	::1	4	LABS-ESTUDIANTES
5	2800	68	21	0	A	0	5	::1	7	TELEFONIA_IP
6	2800	68	21	0	A	0	6	::1	8	SALA_BIBLIOTECA
7	2800	68	21	0	A	0	7	::1	9	SALA_PROFESORES
8	2800	68	21	0	A	0	8	::1	10	WLAN_ESTUDIANTES
9	2800	68	21	0	A	0	9	::1	11	VIDEO-CONFERENCIA
10	2800	68	21	0	A	0	A	::1	12	LAN_SERVIDORES_INTERNOS
11	2800	68	21	0	A	0	B	::1	13	INTERNET-TELCO
12	2800	68	21	0	A	0	C	::1	14	LAN_ELECTRICA
13	2800	68	21	0	A	0	D	::1	18	LAN_INVESTIGACION
14	2800	68	21	0	A	0	E	::1	19	LAN_WLC
15	2800	68	21	0	A	0	F	::1	20	VLAN-DOCENTES
16	2800	68	21	0	A	1	1	::1	21	LABORATORIO_WLAN
17	2800	68	21	0	A	1	2	::1	22	VLAN-COLEGIO-WLAN
18	2800	68	21	0	A	1	3	::1	30	WSA

19	2800	68	21	0	A	1	4	::1	31	PRODUCCION-WSA
20	2800	68	21	0	B	0	1	::1	224	CES-DOCENTES
21	2800	68	21	0	B	0	2	::1	226	CES-COLEGIO
22	2800	68	21	0	B	0	3	::1	228	CES-ESCUELA
23	2800	68	21	0	B	0	4	::1	229	CES-ADM
24	2800	68	21	0	B	0	5	::1	230	CES-SERVER
25	2800	68	21	0	A	1	A	::1	231	WLC-UNIFI
26	2800	68	21	0	A	1	B	::1	232	EVENTOS
27	2800	68	21	0	A	1	C	::1	234	CES-DOCENTE234

Para la asignación del direccionamiento IPv6 en los dispositivos finales se ha escogido seguir con la práctica actual de administración del direccionamiento, que asigna estáticamente una dirección IP a los dispositivos finales servidores, impresoras de red y a las interfaces de los dispositivos se asignan direcciones estáticas y para los otros dispositivos se utilizaran métodos dinámicos (SLACC, DHCPv6).

El proceso de SLACC utiliza las características de mensajes ICMPv6 (NS, NA, RS, RA)

- Solicitación de vecinos NS.
- Anuncio de vecinos NA.
- Solicitación de puerta de enlace RS
- Anuncio de puerta de enlace RA

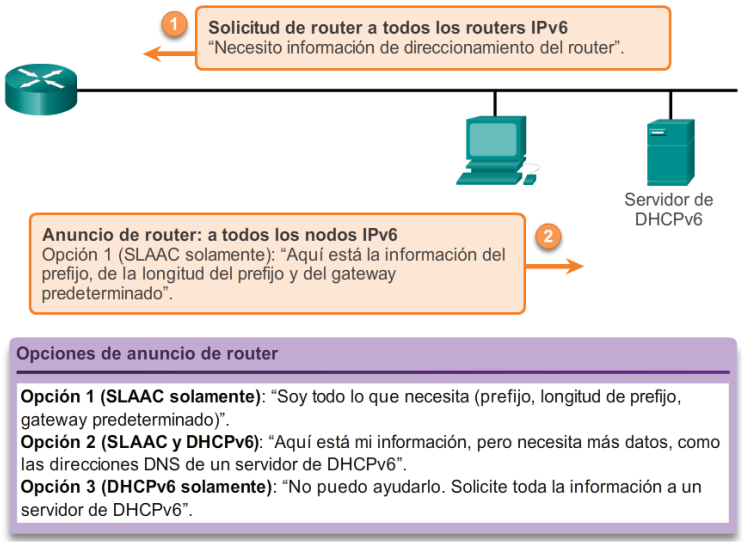


Figura 41. Mensaje de solicitud y anuncio de router (Fuente; Tomado de Cisco Network Academy)

La aplicación de los mensajes ICMPv6 antes descritos son utilizados en el proceso de asignación de dirección, procesos de detección de direcciones duplicadas, valides de dirección y la configuración de la puerta de enlace.

La forma en que SLACC asigna una dirección IPv6 a cada dispositivo final es a través de la asignación del proceso EUI-64 (Proceso de tomar la dirección MAC del equipo, cambiar el bit #7 de cero a uno de los primeros 24 bits del OIU y añadir los 16 bits restantes con FEFE entre los primeros 24 bits correspondientes al OIU y los 24 bits de la interface) o la asignación de un identificador aleatorio (usado principalmente en los equipos con sistema operativo Windows).

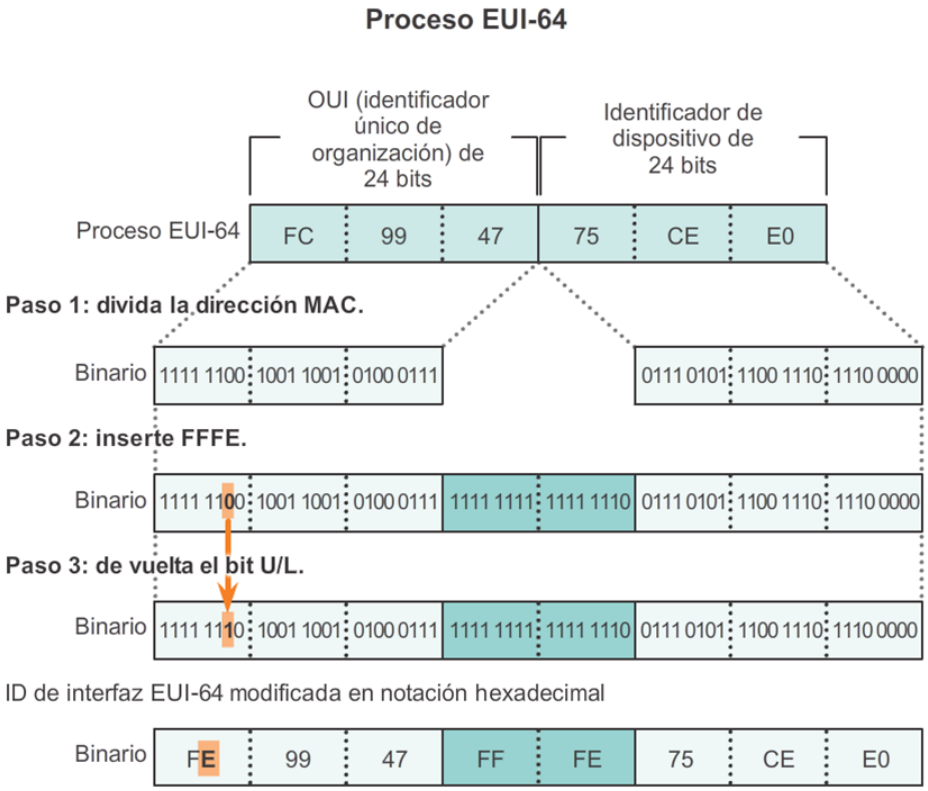


Figura 42. Proceso EUI-64 (Fuente; Tomado de Cisco Network Academy)

4.2.Diseño de estrategias de transición para la UPS de IPv4 a IPv6.

La estrategia escogida para la transición del direccionamiento es la aplicación del modelo DSM que consiste en la implementación de los dos tipos de direccionamiento IPv4 e IPv6.

La ventaja más destacable es la facilidad de implementación y la convivencia de los dos protocolos que trabajaran independientes en la red.

Los equipos que son parte de la infraestructura tecnológica de red en la UPS tienen el soporte para IPv6 por lo que no es necesario realizar técnicas adicionales de traducción de direcciones. En la fase de implementación de IPv6 en la red con el modelo DSM aseguramos que los protocolos mantengan su independencia en operación, permitiendo garantizar un correcto proceso de transición del direccionamiento de IPv4 hacia IPv6.

4.3.Diseño de seguridades en IPv6

La seguridad en IPv6 se fundamentará en el principio de simplicidad y de mantener un esquema de seguridad a profundidad que cubra la seguridad en la frontera de la empresa y la red de campus.

El esquema de seguridad será basado en listas de control de acceso (ACL) que se pueden implementar en los equipos de la UPS y en el prototipo a ejecutarse.

Se seguirán las funciones y características de seguridad de primer salto (FHS) diseñadas para robustecer la operación proporcionando una sólida protección en escenarios de implementación de IPv6.

4.3.1. Red de campus.

El modelo de seguridad se puede analizar en la red de campus en tres posiciones. Puede ser aplicada en los dispositivos finales, en el primer salto en la red y en el último salto, permitiendo la posibilidad de robustecer la política de seguridad en un esquema de profundidad.

Figura 43. Esquema de seguridad de profundidad (Fuente; el autor)

En la red de campus la configuración está dirigida a evitar ataques que se produzcan a causa de equipos no autorizados que suplanten las funciones de enrutadores o de servicios que faciliten vectores de ataque desde dentro de la red como los denominados de hombre en el medio (MiM) como se puede ver en el esquema de la figura 42.

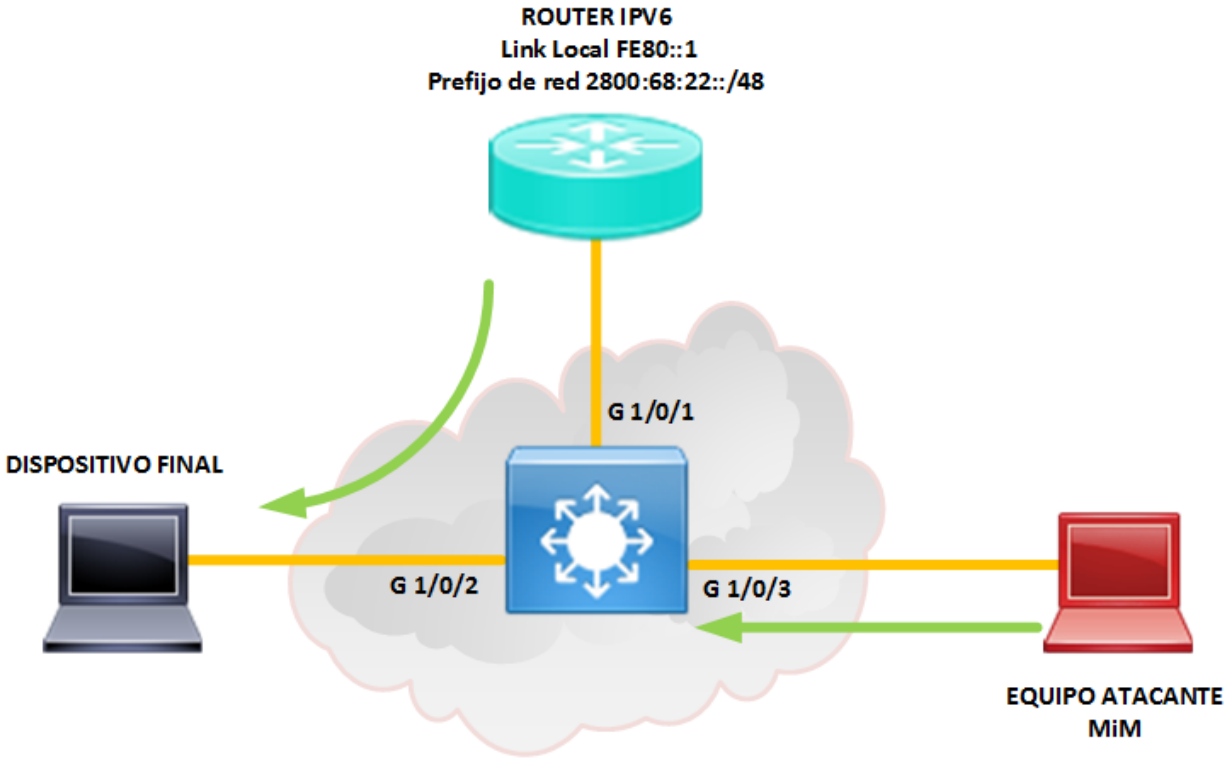


Figura 44. Esquema de uso de RA para hacer un ataque de MiM. (Fuente; El autor)

La característica para la red de campus RA GUARD permite al administrador de la red bloquear o rechazar los mensajes de anuncio de puerta de enlace RA que permiten a los

dispositivos anunciarse en la red. RA GUARD permite identificar el rol que tendrá los dispositivos conectados a la interface de red (host o router) a través de políticas y con configuraciones avanzadas permitir únicamente a los dispositivos y al prefijo de red autorizados por el administrador.

La protección al aplicar la característica de RA GUARD entre sus principales funciones son:

- Verificación de la integridad de la dirección.
- Protecciones de los mensajes RA
- Autorización de equipos en la red para compartir los prefijos de red IPv6

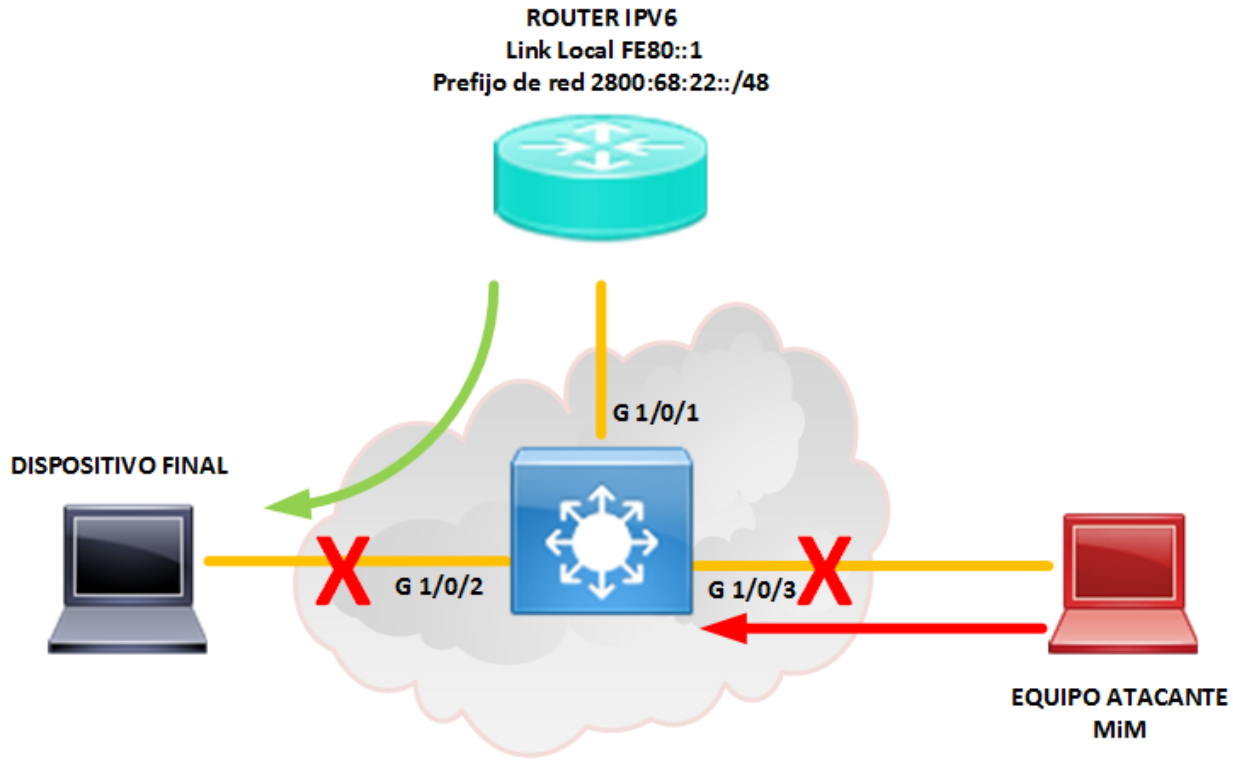


Figura 45. Esquema de funcionamiento de RA GUARD (Fuente; El autor)

En la figura 43 se muestra la aplicación de RA GUARD en las interfaces G1/0/1, G1/0/2 y G1/0/3, para las interfaces (G1/0/2 y G1/0/3) se ha configurado el comando **ipv6 nd raguard** que descartara cualquier intento de que por las interfaces habilitadas con el comando se envié

mensajes RA**.** En la interface G1/0/1 no se habilita el comando por lo que por esta interface si se acepta el intercambio de mensajes RA.

El modo de aplicar esta función puede variar y fundamentarse en el control especifico con la creación de listas de control de acceso que facilite la implementación directa a toda una VLAN y no a la configuración de un puerto es especial.

Para el caso de la implementación de RA GUARD basada en una política deberemos identificar al router que será el permitido a través de su dirección de enlace local (link local) y por el prefijo de red IPv6 que será permitido en los mensajes RA, los datos para el ejemplo serán los que se encuentran en la figura 43 con los comandos:

- **ipv6 access-list "nombre de ACL"** (definición de la ACL para permitir al router)
    - *permit ipv6 host "dirección de enlace local" any* (permitir IPv6 del router)

Ejemplo:

```
switch> enable
switch# configure terminal
switch(config)# ipv6 access-list ROUTER-IPV6
switch(config-ipv6-acl)#permit ipv6 host fe80::1 any
switch(config-ipv6-acl)#exit
```

- **ipv6 prefix-list "nombre del prefijo" permit "prefijo IPv6"** (permitir el prefijo IPv6)

Ejemplo:

```
switch(config)# ipv6 prefix-list PREFIJO-IPV6 permit 2800:68:22::/48
```

- **ipv6 nd raguard policy "nombre de la política"** (nombre de la política para RA GUARD)
    - *device-role router*
    - *match ipv6 access-list "nombre de ACL para permitir el router"*

- *match ra prefix-list "nombre del prefijo IPv6"*

Ejemplo:

```
switch(config)# ipv6 nd raguard policy POLITICA-RA
switch(config-ra-guard)# device-role router
switch(config-ra-guard)# match ipv6 access-list ROUTER-IPV6
switch(config-ra-guard)# match ra prefix-list PREFIJO-IPV6
```

Una vez definida la política esta se debe aplicar a la interface del switch donde está conectado el router que en nuestro caso es la interface G1/0/1 ingresando al modo de configuración de la interface y aplicar el comando **ipv6 nd raguard attach-policy "nombre de la política"**

Ejemplo:

```
switch> enable
switch# configure terminal
switch(config)# interface G 1/0/1
switch(config-if)# ipv6 nd raguard attach-policy POLITICA-RA
```

Para el caso de los dispositivos finales se aplicará la configuración de RA GUARD a toda la VLAN para lo que se deberá crear una política que defina el rol de dispositivo final con los siguientes comandos:

- **ipv6 nd raguard policy "nombre de la política"** (nombre de la política para RA GUARD)
  - *device-role host*

Ejemplo:

```
switch(config)# ipv6 nd raguard policy PARA-HOST
switch(config-ra-guard)# device-role host
```

Se debe aplicar la política en el switch para que funcione en toda una VLAN y no hacerlo por puerto, por lo que la solución de implementación tiene una posibilidad de escalamiento mejorada al usar la característica de políticas fundamentadas en ACL para el control de la característica de

RA GUARD. La aplicación se la debe realizar directamente a la VLAN que para el ejemplo se usara el ID 112.

Ejemplo:

```
switch> enable
switch# configure terminal
switch(config)#vlan configuration 112
switch(config-vlan-config)#ipv6 nd raguard attach-policy PARA-HOST
```

4.3.2. Red de frontera.

Las seguridades en frontera de la empresa serán aplicadas en base a filtros fundamentados en listas de control de acceso (ACL) que permitan o denieguen los diferentes flujos de información hacia el internet y en la distribución, considerando el perfil y la funcionalidad de cada subred que deba tener según las necesidades de la UPS.

Las ACL en IPv6 son de tipo nombradas, tienen las mismas características que en IPv4 que fundamentan sus reglas basadas en las redes de origen y destino del tráfico y se deben asignar a una interface en sentido del flujo de información que se desea filtrar de entrada o salida.

Las ACL son una estructura jerárquica donde el orden de la declaración de las redes es importante, una ventaja significativa de las ACL en IPv6 nombradas es que se pueden hacer modificaciones en el orden de las reglas declaradas a través del número de secuencia.

Otra característica que se debe considerar es la inclusión de reglas implícitas en la creación de las ACL de IPv6, son tres reglas que se encuentran implícitas en la utilización de ACL que son:

- permit icmp any any nd-na
- permit icmp any any nd-ns
- deny any any

Las reglas ND son las que se utilizan en el proceso de descubrimiento de vecinos que es parte fundamental en auto configuración de IPv6. La regla deny any any es la regla implícita al final que hace que las ACL descarten todo el tráfico que no se haya definido como permitido en la descripción de las sentencias anteriores.

Los comandos para permitir o denegar un flujo de información son:

- **ipv6 access-list "NOMBRE-ACL"** (Define el nombre de la ACL de IPv6)
    - *permit/deny "protocolo" "origen de tráfico" "destino de tráfico" "operador lógico" "numero de puerto" (inclusión de algunas opciones avanzadas)*

Ejemplo:

```
routerIPv6> enable
routerIPv6# configure terminal
routerIPv6(config)# ipv6 access-list NAVEGACION
routerIPv6(config-ipv6-acl)#permit tcp host 2800:68:22:A01::1 any eq 80
routerIPv6(config-ipv6-acl)#permit tcp host 2800:68:22:A01::1 any eq 443
routerIPv6(config-ipv6-acl)#permit udp host 2800:68:22:A01::1 any eq 53 log
```

El paso final para que la ACL creada pueda iniciar a operar es asignarla a una interface, las ACL en IPv6 utilizan el comando traffic-filter y la dirección en que se desea filtrar los flujos de información (in / out).

- **ipv6 traffic-filter (nombre de ACL) (in/out)**
-

Ejemplo:

```
SwitchIPv6(config)#interface vlan 112
SwitchIPv6(config-if)#ipv6 traffic-filter NAVEGACION in
```

Para facilitar la implementación de ACL es recomendable utilizar una tabla que nos permita visibilizar y organizar los parámetros a controlar, que nos dará como resultado el formato de las

sentencias y el orden en que la ACL se deberá configurar el ejemplo de cómo usar esta recomendación estará en la tabla 21.

Tabla 24.
Guía de ejemplo para la creación de ACL IPv6 (Fuente; El autor)

ACCION	PROTOCOLO	ORIGEN	DESTINO	OPERADOR	PUERTO
permit	tcp	host 2800:68:22:A29::2	any	eq	80
permit	tcp	host 2800:68:22:A29::3	any	eq	443
permit	tcp	host 2800:68:22:A29::4	any	range	21 25
permit	tcp	host 2800:68:22:A29::5	any	lt	5000
permit	tcp	host 2800:68:22:A29::5	any	gr	6000
deny	icmp	2800:68:22:C01::/64	host 2800:68:22:A29::5	neq	23

4.4.Implementación de prototipo en el Campus El Girón.

La implementación del prototipo configuraremos en la infraestructura de producción, aprovechando que el modelo SDM nos permite mantener los dos protocolos en la infraestructura de red y mantener total independencia en la operación de IPv6 y de IPv4.

Los equipos que se usaran en el prototipo son los equipos de distribución de la red de campus en modelo colapsado Cisco catalyst WS-6506-E y el router 3851. La topología a usarse en la implantación del prototipo se describe en la figura 44.

4.4.1. Implementación en red de campus.

La implementación del prototipo en la red de campus El Girón consistirá en la configuración del equipo Cisco catalyst WS-6506-E al que se le configurará las direcciones IPv6 de la tabla 20 en las interfaces virtuales conmutadas SVI, se habilita la configuración básica necesaria para la operación del protocolo IPv6 con el comando **ipv6 unicast-routing** y funcionalidades de FHS.

Ejemplo: Configuración de dual stack en SVI de la VLAN3

```
interface Vlan3
 description "VLAN administrativa"
 ip address 172.17.3.252 255.255.254.0
 ipv6 address 2800:68:22:A02::1/64
```

ipv6 dhcp server IPv6-DNS-SW
end

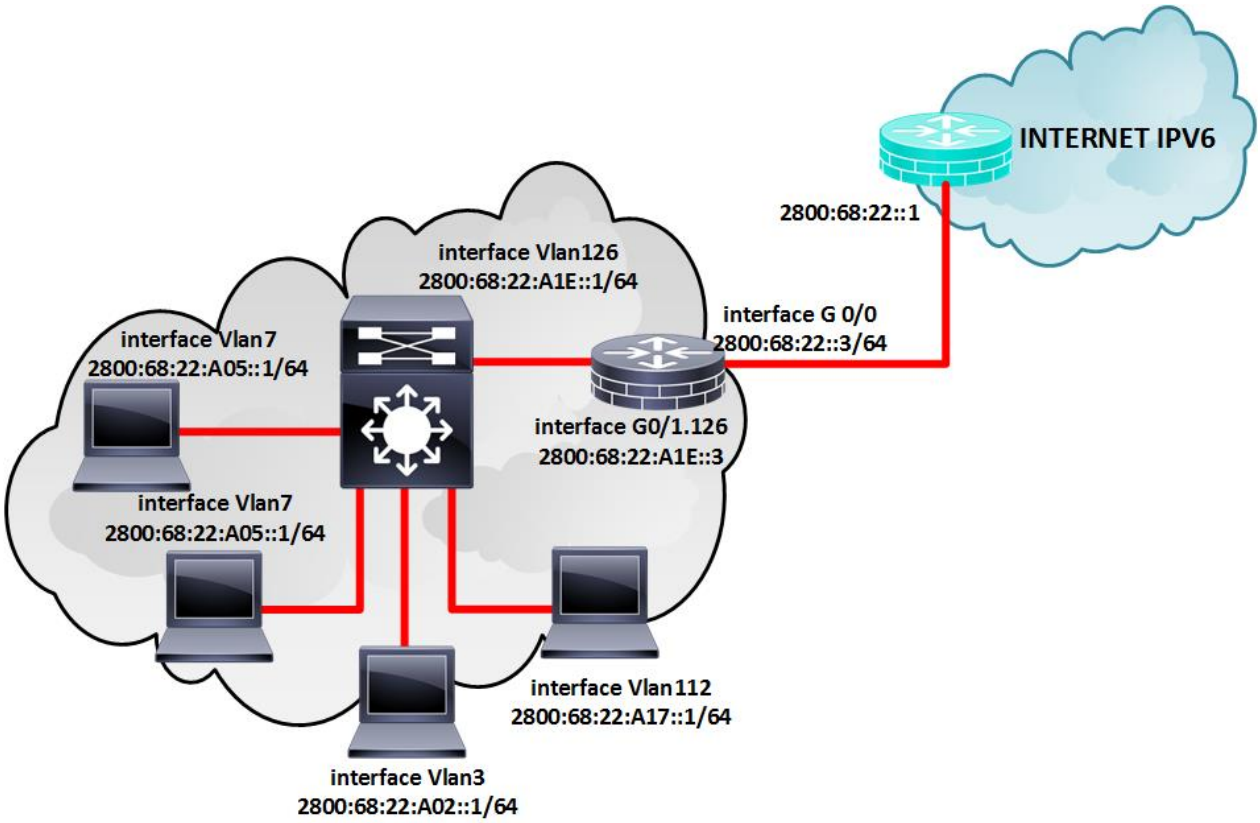


Figura 46. Topología del prototipo implementado en El campus El Girón (Fuente; El autor)

```
interface vlan3
 description "VLAN administrativa"
 ip address 172.17.3.252 255.255.254.0
 ipv6 address 2800:68:22:A02::1/64
 ipv6 dhcp server IPv6-DNS-SW
end
```

Figura 47.Configuración IPv6 SVI VLAN 3 (Fuente; El autor)

Con el comando: **sh run | section include ipv6** nos permitirá visibilizar la configuración IPv6 aplicada en el equipo de distribución Cisco catalyst WS-6506-E.

Ejemplo:

MDF-B#sh run | section include ipv6

```
ipv6 unicast-routing
ipv6 dhcp pool IPv6-DNS-SW
 dns-server 2001:4860:4860::8888
 domain-name ups.edu.ec
ipv6 multicast rpf use-bgp
class-map match-all class-copp-mcast-ipv6-control
class-map match-any class-copp-ipv6-connected
  class class-copp-ipv6-connected
    police rate 1000 pps burst 256 packets    conform-action transmit     exceed-action drop
 ipv6 nd raguard
 ipv6 address 2800:68:22:A01::1/64
 ipv6 address 2800:68:22:A02::1/64
 ipv6 dhcp server IPv6-DNS-SW
 ipv6 address 2800:68:22:A03::1/64
 ipv6 address 2800:68:22:A04::1/64
 ipv6 address 2800:68:22:A05::1/64
 ipv6 address 2800:68:22:A07::1/64
 ipv6 address 2800:68:22:C01::1/64
 ipv6 address 2800:68:22:A0A::1/64
 ipv6 address 2800:68:22:D01::1/64
 ipv6 address 2800:68:22:B01::1/64
 ipv6 address 2800:68:22:F01::1/64
 ipv6 address 2800:68:22:A1B::1/64
 ipv6 address 2800:68:22:A1E::1/64
 ipv6 address 2800:68:22:A29::1/64
 ipv6 address 2800:68:22:A2B::1/64
ipv6 route ::/0 2800:68:22:A1E::3
ipv6 access-list acl-copp-match-mld
 permit icmp any any mld-report
 permit icmp any any mld-query
 permit icmp any any mld-reduction
 permit icmp any any 143
ipv6 access-list acl-copp-match-ndv6
 permit icmp any any nd-na
 permit icmp any any nd-ns
 permit icmp any any router-advertisement
 permit icmp any any router-solicitation
 permit icmp any any redirect
ipv6 access-list acl-copp-match-pimv6-data
 deny 103 any host FF02::D
 permit 103 any any
```

Se realiza una prueba de la operación del protocolo IPv6 en la red de campus con protocolos ping, show ipv6 neighbors y traceroute

Ejemplo: comando PING

MDF-B#ping 2800:68:22:A1E::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:22:A1E::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms

```
MDF-B#ping 2800:68:22:A1E::3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:22:A1E::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
```

Figura 48. Resultado ejecución comando ping (Fuente; El autor)

```
MDF-B#sh ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
2800:68:22:A1B:582D:61F2:6A01:5F8F           0 0050.568b.3bb1  STALE Vl119
FE80::E0BE:338:74B6:ABBF                     0 50b7.c389.771f  STALE Vl14
2800:68:22:A02:F14B:62F2:DBD8:293B           5 4c72.b921.1900  STALE Vl3
2800:68:22:A2B:250:56FF:FE8B:625F           51 0050.568b.625f  STALE Vl830
FE80::5C1F:2FE1:D351:270D                    1 e069.9589.4625  STALE Vl14
FE80::225:B3FF:FEF2:C48F                     1 0025.b3f2.c48f  STALE Vl3
2800:68:22:A0A:20C:29FF:FEAD:B239           15 000c.29ad.b239  STALE Vl13
2800:68:22:A29:4DF9:4623:8597:C707          11 0050.56bd.7620  STALE Vl810
2800:68:22:D01:F6CE:46FF:FE33:8D62           2 f4ce.4633.8d62  STALE Vl14
2800:68:22:A02:2445:DCE:D921:B8CE            0 9890.96b3.c35f  STALE Vl3
2800:68:22:A29:74F3:4734:3D13:487            1 0050.568b.3d4a  STALE Vl810
2800:68:22:A02:ED2A:C31A:2F28:A566          27 9890.96b4.4273  STALE Vl3
FE80::217:59FF:FE0E:3C51                     0 0017.590e.3c51  REACH Vl126
2800:68:22:A02:4939:7E2:17:1DC4              4 047d.7b3d.5df9  STALE Vl3
FE80::1A5:E0A0:F864:D3AA                    60 9890.96b4.767f  STALE Vl3
2800:68:22:A04:8998:7D61:9FB1:554B          49 9890.96b3.c4cb  STALE Vl3
2800:68:22:A2B:250:56FF:FE8B:6810           10 0050.568b.6810  STALE Vl830
2800:68:22:A0A:FA0F:41FF:FE56:D5B0           4 f80f.4156.d5b0  STALE Vl13
2800:68:22:A1E::3                            0 0017.590e.3c51  REACH Vl126
2800:68:22:A1B:6464:B5A3:C424:4CEB           0 0050.568b.7013  STALE Vl119
FE80::AA7C:1FF:FECC:9A93                   214 a87c.01cc.9a93  STALE Vl14
FE80::D062:4F28:D54A:92DC                    4 54be.f708.da8a  STALE Vl14
2800:68:22:D01:250D:27F4:7E91:E941           0 001c.c0b8.b8f9  REACH Vl14
```

Figura 49. Ejecución del comando sh ipv6 neighbors (Fuente; El autor)

Finalmente, la configuración de IPv6 en switch es configurar una ruta por defecto a la puerta de enlace conectada hacia el router 3851, para que la red del campus pueda salir al internet IPv6.

El comando usado es ipv6 route ::/0 2800:68:22:A1E::3

```
MDF-B#sh ipv6 route
IPv6 Routing Table - default - 30 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via 2800:68:22:A1E::3
C   2800:68:22:A01::/64 [0/0]
     via Vlan1, directly connected
L   2800:68:22:A01::1/128 [0/0]
     via Vlan1, receive
C   2800:68:22:A02::/64 [0/0]
     via Vlan3, directly connected
L   2800:68:22:A02::1/128 [0/0]
     via Vlan3, receive
C   2800:68:22:A03::/64 [0/0]
     via Vlan4, directly connected
L   2800:68:22:A03::1/128 [0/0]
     via Vlan4, receive
C   2800:68:22:A04::/64 [0/0]
     via Vlan6, directly connected
```

Figura 51. Ejecución del comando ipv6 route (fuente; El autor)

4.4.2. Implementación en frontera de la empresa.

En la frontera para que la conexión a internet IPv6 funcione nos conectamos con el router del proveedor CEDIA a la dirección IPv6 2800:68:22::1. Configuramos en la interface GigabitEthernet0/0 configuramos una dirección IPv6 del mismo segmento, y configuramos la dirección IPv6 2800:68:22::3/64 con el comando ipv6 address, como se muestra en la figura 50.

```
interface GigabitEthernet0/0
 description #### LINK  TO ISP ####
 ip address 190.95.172.40 255.255.255.224
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 media-type rj45
 ipv6 address 2800:68:22::3/64
 no keepalive
```

Figura 52. Configuración Interface G 0/0 (Fuente; El autor)

Para la conexión con la red de campus entre el equipo switch WS-6506-E y la frontera de la empresa con equipo router 3851 creamos subinterfaces y configuramos direcciones IPv6 como se muestra en la figura 51.

```
interface GigabitEthernet0/1.112
 description #### VLAN ADMIN ####
 encapsulation dot1Q 112
 ip address 172.17.113.252 255.255.254.0
 ip nat inside
 ip virtual-reassembly
 ipv6 address 2800:68:22:A17::2/64
 ipv6 address FE80::1 link-local
 ipv6 dhcp server IPv6_DNS
!
interface GigabitEthernet0/1.126
 description #### VLAN INTERNET ####
 encapsulation dot1Q 126
 ip address 172.17.126.253 255.255.255.0
 ipv6 address 2800:68:22:A1E::3/64
 ipv6 dhcp server IPv6_DNS
```

Finalmente utilizamos las características de enrutamiento para crear una ruta por defecto hacia el proveedor y rutas estáticas hacia dentro de la red. La ruta por defecto debe tener como próximo salto la dirección IPv6 2800:68:22::1 y la estática que permitirá alcanzar las redes de campus es la dirección IPv6 2800:68:22:A1E::1.

La configuración de rutas estáticas se muestra en la figura 52.

```
ipv6 route 2800:68:22::/48 2800:68:22:A1E::1
ipv6 route ::/0 2800:68:22::1
```

Figura 54. Configuración de rutas estáticas (Fuente; El autor)

En la figura 53 se muestra la tabla de enrutamiento IPv6 del router 3851.

Una vez aplicadas las configuraciones revisamos que el protocolo esté funcionando con los comandos básicos de diagnóstico ping, traceroute. Desde el router validaremos con ping la conexión a la puerta de enlace de CEDIA, interface del switch WS-6506-E y luego conexión

```
RT-UPS-UIOG#SH IPV6 ROUte
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via 2800:68:22::1
S   2800:68:22::/48 [1/0]
     via 2800:68:22:A1E::1
C   2800:68:22::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2800:68:22::3/128 [0/0]
     via ::, GigabitEthernet0/0
C   2800:68:22:A17::/64 [0/0]
     via ::, GigabitEthernet0/1.112
L   2800:68:22:A17::2/128 [0/0]
     via ::, GigabitEthernet0/1.112
C   2800:68:22:A1E::/64 [0/0]
     via ::, GigabitEthernet0/1.126
L   2800:68:22:A1E::3/128 [0/0]
     via ::, GigabitEthernet0/1.126
L   FE80::/10 [0/0]
     via ::, Null0
```

Figura 55. Rutas IPv6 router 3851 (Fuente, El Autor)

hacia el internet a los DNS de google las direcciones IPv6 2001:4860:4860::8888 y

2001:4860:4860::8844 el resultado exitoso de la conexión de la UPS con el internet en versión IPv6 a través del comando ping se muestra en la figura 54.

```
RT-UPS-UIOG#ping 2800:68:22::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:22::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
RT-UPS-UIOG#ping 2800:68:22:A1E::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:22:A1E::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
RT-UPS-UIOG#ping 2001:4860:4860::8844

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:4860:4860::8844, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/68/68 ms
RT-
```

Figura 56. Resultado de ping IPv6 en router 3851 (Fuente; El autor)

EL resultado de realizar traceroute hacia los DNS de google se mostrará en la figura 55.

```
RT-UPS-UIOG#traceroute 2001:4860:4860::8888

Type escape sequence to abort.
Tracing the route to 2001:4860:4860::8888

  1 2800:68:22::1 4 msec 0 msec 0 msec
  2 2800:2A0:21:211::1 0 msec 0 msec 4 msec
  3 ::FFFF:10.201.21.226 8 msec 8 msec 8 msec
  4 ::FFFF:10.201.111.145 8 msec 8 msec 8 msec
  5 2800:2A0:11:30::1 8 msec 8 msec 8 msec
  6 2800:2A0:11:30::3 12 msec 12 msec 12 msec
  7 2800:2A0:11:11:1::39 68 msec 68 msec 68 msec
  8 2001:4860:0:1::130A 68 msec
    2001:4860:0:1::1312 72 msec
    2001:4860:0:1::130E 68 msec
  9 2001:4860:0:1::109E 68 msec
    2001:4860:0:1::1216 72 msec
    2001:4860:0:1::1086 68 msec
 10 2001:4860:4860::8888 68 msec 68 msec 72 msec
```

Figura 57. Resultado de una traza hacia DNS de google (Fuente; El autor)

Una vez configurado todo en el prototipo iniciamos la revisión del éxito de navegación al internet con IPv6 en los dispositivos finales.

Las pruebas se realizaron navegando en portales de validación de IPv6 y en sitios listos para IPv6. Para la verificación de la dirección IP en que se navega y verificar si los sitios tienen capacidad para responder a contenido IPv6, se habilitaron las extensiones del navegador Mozilla Firefox de nombre Show IP que es un complemento que habilita una barra de herramienta que permiten ver las direcciones IP que se visita y otra información relevante de los sitios en los navegadores.

En la figura 56, se muestra el resultado de navegar en el sitio ipv6.google.com

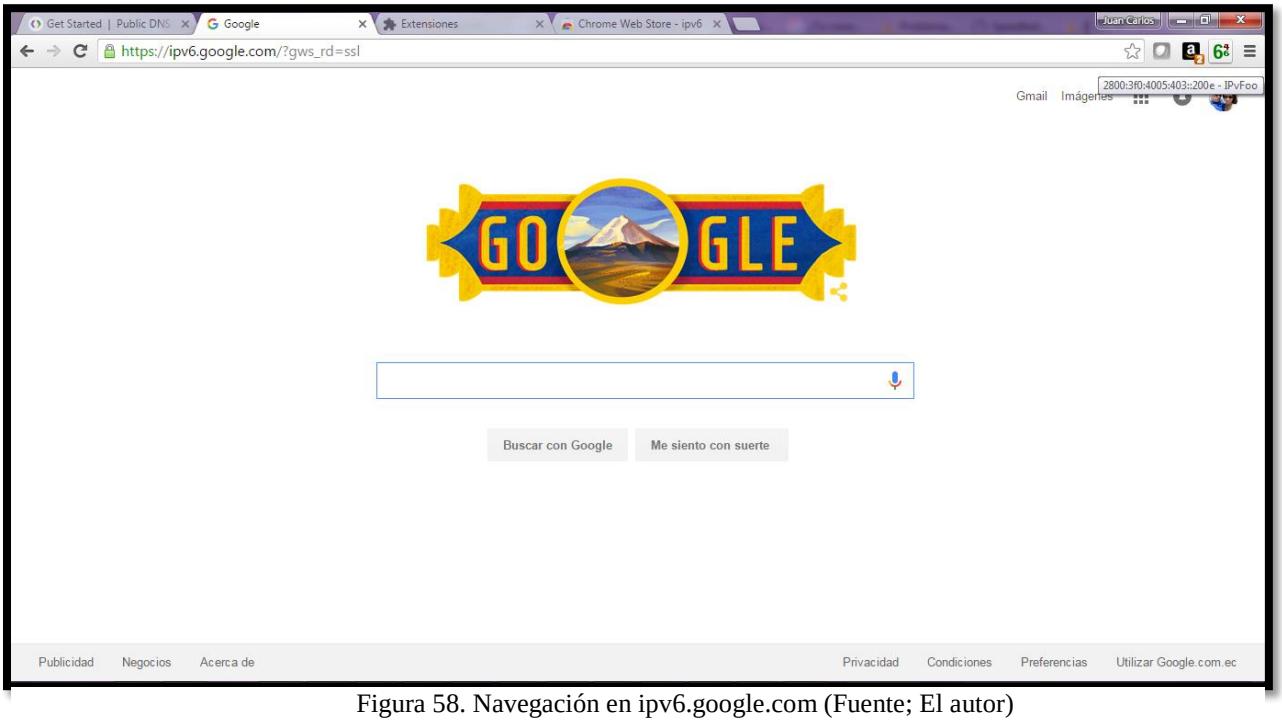


Figura 58. Navegación en ipv6.google.com (Fuente; El autor)

En la figura 57. Se muestra el resultado de navegar en el sitio ipv6-test.com donde nos muestra la direccion IPv6 de un dispositivo final de la VLAN 112 2800:68:22:a17:852b:caa0:a5d3:d8ed y la direccion IPv4 configurada en el equipo de frontera router cisco 3851.

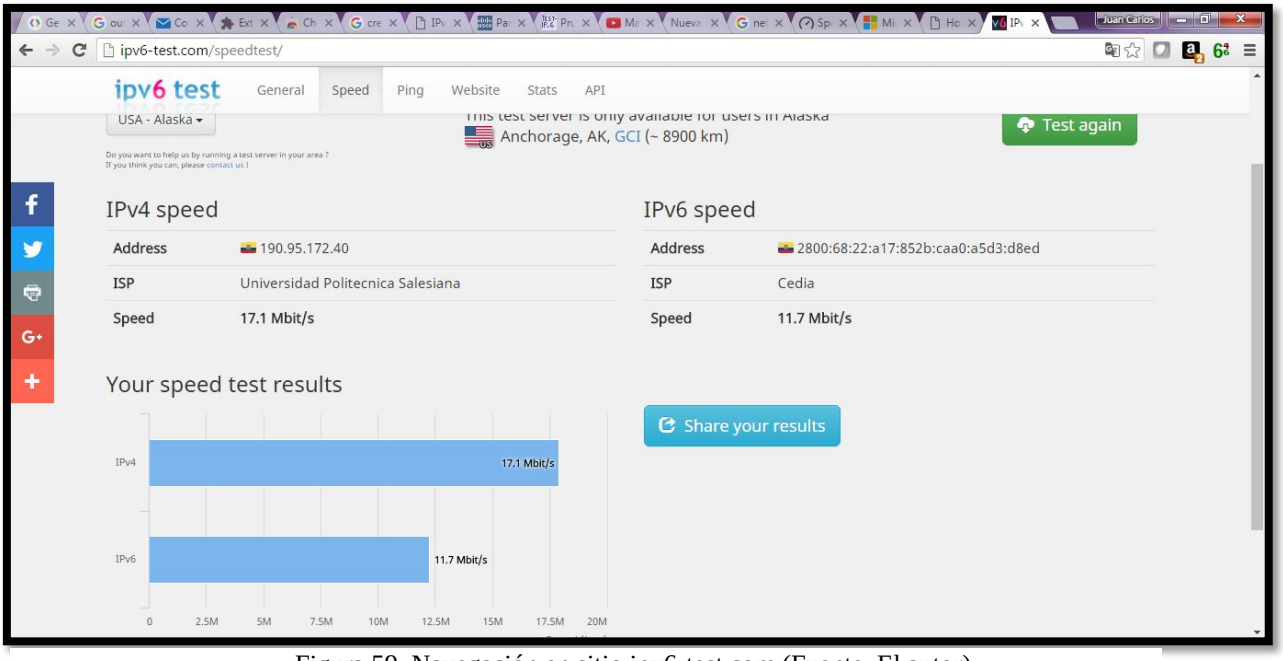


Figura 59. Navegación en sitio ipv6-test.com (Fuente, El autor)

En la figura 58 se muestra la navegacion de otra direccion IPv6 de un dispositivo final de la VLAN 112.

Figura 60. Navegación en sitio get.youripfast.com (Fuente; El autor)

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

El desarrollo de este trabajo pasa de un alcance académico teórico a la aplicación de configuraciones IPv6 en una red de producción, utilizando un segmento de la red para crear un prototipo del funcionamiento del modelo de doble pila (DSM), y lograr navegación a internet a través del protocolo IPv6. La implementación de IPv6 en la red de la UPS ofrece una posibilidad de soporte a las nuevas tendencias y retos actuales de las redes de comunicaciones.

Con el levantamiento de la información de la infraestructura de red actual de la UPS se verificó el soporte de las características de IPv6, lo que facilitó la elección del método de transición de IPv4 a IPv6. Se consiguió la independencia de la operación del prototipo implementado en IPv6 sin afectar la infraestructura actual de versión IPv4, lo que fue transparente para los dispositivos finales y los usuarios de la UPS. No fue necesario la utilización de métodos adicionales o modelos híbridos para la implementación del prototipo.

El modelo jerárquico empresarial permitió la identificación de la línea base de la red e identificar los roles de los dispositivos que estarán usados en la implementación del prototipo. La metodología PPDIOO escogida para el diseño, garantiza que el resultado obtenido esté dentro de los requerimientos iniciales y sea posible un seguimiento a la operación y de ser necesario considerar propuestas de mejoras al diseño.

El plan IPv6 diseñado fue realizado con direcciones unicast globales que permiten tener visibilidad directa entre el dispositivo de origen del tráfico y el dispositivo destino del flujo de tráfico; se revisó la cantidad de subredes y las unidades organizacionales que componen a la UPS en cada campus para poder crear la asignación de direcciones IPv6 y mostrar la jerarquía del direccionamiento. Para la creación del plan IPv6 se solicitó al ISP CEDIA la asignación de prefijos globales de enrutamiento para los campus Sur (2800:68:16::/48), El Girón (2800:68:22::/48) y Kennedy (2800:68:21::/48); se usó el hexteto restante de la porción de red

para demostrar la jerarquía del direccionamiento y finalmente para la asignación de direcciones IP para los dispositivos finales se usa el método de configuración dinámico sin estado.

La implementación del prototipo en una red de producción permitió visibilizar claramente que características de IPv6 se debe configurar en los dispositivos para lograr navegar exitosamente a internet con el uso de IPv6. En la implementación se pudo comprobar que a la falta de implementaciones de redes con IPv6 el soporte de los ISP y otras instancias tardan mucho en resolver problemas aparentemente no complejos como los de enrutamiento global de los prefijos. La habilitación de seguridad fundamentada en FHS con la característica RA GUARD mitigará ataques de suplantación y ayudará a optimizar el consumo de recursos de CPU en los dispositivos finales. Las ACL en IPv6 no tienen un cambio en su estructura en contraste con las ACL de IPv4; se recomienda considerar únicamente incluir las características de reglas implícitas propias del protocolo IPv6.

BIBLIOGRAFÍA:

- Álvaro Vives, Mariela Rocha, Jordy Palet, César Olvera Morales, Christian O'Flaherty , Roque Galiano, G. C. (2009). Ipv6 para todos. Internet Society.
- Babiker, H., Nikolova, I., & Chittimaneni, K. K. K. (2011). Deploying IPv6 in the Google Enterprise Network. Lessons learned. LISA'11 Proceedings of the 25th International Conference on Large Installation System Administration, 10. doi:December, 2011.
- Blanchet, M. (2006). Migrating to IPv6. John Wiley & Sons, Ltd. Québec, Canada. doi:10.1002/9780470028742.
- Cisco System, I. (2011). Deploying IPv6 in Campus Networks. Cisco Validate Design, (Abril), 40. Retrieved from http://www.cisco.com/web/strategy/docs/gov/IPv6CampusNetwork.pdf
- Cisco System, I. (2012). Deploying IPv6 in Campus Networks. Cisco Validate Design, (Febrero), 59. Retrieved from http://www.cisco.com/web/strategy/docs/gov/IPv6CampusNetwork.pdf.
- Cisco System, I. (2013). Table of of contents. Cisco Validate Design, (Agosto), 43. doi:10.1002/ejoc.201200111
- Cisco System, I. (2014). IPv6 DMZ Web Service Table of Contents. Cisco Validate Design, (August), 32.
- Jonas, K., Idris A., R., & Tchuente, M. (2012). e- Infraestructure and e- Services for Developing Countries. Springer.
- Racherla, S., & Daniel, J. (2013). Front cover IPv6 Introduction and Configuration. IBM, 96.